Livingston
Enterprises, Inc.

PortMaster2
User's Manual

PM-2 & PM-2e
Communications Server

PortMaster2
User's Manual

PM-2 & PM-2e
Communications Server

Part No. 950-1103F Printed in U.S.A. 1/94

REVISION HISTORY

First Edition.....Release 1.1.....9/89

Second Edition.....Release 2.0.....7/90

Third Edition.....Release 2.1.....11/90

Fourth Edition.....Release 2.3.....8/92

Fifth Edition.....Release 2.4.....10/93

Sixth Edition.....Release 3.0.....1/94

NOTICE

The information contained in this document is subject to change without notice.

Livingston Enterprises, Inc. makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Livingston Enterprises, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance or use of this material.

This document contains proprietary information which is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced or translated to another language without the prior written consent of Livingston Enterprises, Inc.

Copyright © 1989-1994 by Livingston Enterprises, Inc.

FCC WARNING

This equipment has been tested and has been found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation in a residential area may cause unacceptable interference to radio and TV reception requiring the operator, at his own expense, to take whatever steps are necessary to correct the interference.

TRADEMARKS

PortMaster is a trademark of Livingston Enterprises, Inc.

OpenWindows is a trademark of Sun Microsystems, Inc.

Open Look is a trademark of AT&T.

Table of Contents

CHAPTER 1, Introduction 1-1
Operating Modes 1-2
Smart Features 1-3
About This Manual 1-3
New features in this release 1-5
Requesting Assistance 1-6

CHAPTER 2, Installation 2-1
Hardware Installation 2-1
Connecting Serial Devices 2-6
Connecting Parallel Devices 2-7
Connecting the Ethernet 2-8
Workstation Software Installation 2-9
PortMaster Internet Address Setup 2-13

CHAPTER 3, Administration under X-Windows 3-1
PortMaster Console 3-1
pmconsole with X-Windows 3-2
PortMaster Login 3-3
Global Configuration 3-4
Ethernet Port Configuration 3-8
Installation from PortMaster Console 3-11
Serial Port Configuration 3-12
Serial Port Parameters 3-14
Standard Mode Parameters 3-15
Extended Mode Parameters 3-18
Hardwired Dialnet parameters 3-23

Parallel Port Configuration 3-26
Managing the Hosts Table 3-27
Managing the Users Table 3-29
Login User Parameters 3-31
Network User Parameters 3-33
Managing the Location Table 3-38
Location Table Parameters 3-39
Dialing Out to Remote Locations 3-45
Managing the Routes Table 3-48
Packet Filters 3-50
Managing the Filter Table 3-51
IP Rules 3-53
IPX Rules 3-55
SAP Rules 3-56
Filter Table Example 3-57
Configuring SNMP 3-58
RADIUS 3-62
Monitoring the PortMaster 3-63
CHAPTER 4, Administration with an ASCII Terminal 4-1
PortMaster Login 4-2
Global Configuration 4-4
Ethernet Port Configuration 4-8
Installation from PortMaster Console 4-11
Serial Port Configuration 4-12
Serial Port Parameters 4-13
Standard Mode Parameters 4-14
Extended Mode Parameters 4-17
Hardwired Dialnet Parameters 4-22
Parallel Port Configuration 4-25
Managing the Hosts Table 4-26

Managing the Users Table 4-27
Login User Parameters 4-29
Network User Parameters 4-30
Managing the Location Table 4-35
Location Table Parameters 4-36
Dialing Out to Remote Locations 4-43
Managing the Routes Table 4-46
Packet Filters 4-47
Managing the Filter Table 4-50
IP Rules 4-52
IPX Rules 4-54
SAP Rules 4-55
Filter Table Example 4-56
Configuring SNMP 4-57
SNMP Parameters 4-58
RADIUS 4-60
Monitoring the PortMaster 4-62
CHAPTER 5, Command Prompt Interface 5-1
The User Commands 5-1
Using the Commands 5-2
Managing Global Parameters 5-3
Managing Ethernet Parameters 5-5
Managing Port Configurations 5-7
Setting the Serial Port Type 5-7
Setting Port Parameters 5-9
Setting Dialnet Hardwired Port Parameters 5-15
SHOW Command 5-17
IFCONFIG Command 5-20
PING Command 5-21
PTRACE Command 5-21

RLOGIN Command 5-22
TELNET Command 5-22
TRACEROUTE Command 5-23
QUIT, DONE, EXIT Command 5-23
HELP Command 5-23
Managing the Hosts Table 5-24
Managing the Users Table 5-27
Setting Login User Parameters 5-29
Setting Network User Parameters 5-30
Managing the Location Table 5-35
Managing the Routes Table 5-41
Dialing Out to Remote Locations 5-43
Packet Filters 5-45
Filter Creation 5-47
IP Rules 5-47
IPX Rules 5-50
SAP Rules 5-51
Packet Processing 5-52
Ethernet Interface Filters 5-53
Hardwired Serial Interface Filters 5-53
Dial-In User Filters 5-54
Dial-Out Location Filters 5-54
Filter Examples 5-55
Configuring SNMP 5-58
CHAPTER 6, RADIUS 6-1
Introduction 6-1
Installation 6-1
Administration 6-1
User Service Types 6-2
Attribute/Value Pairs 6-3

Users file examples 6-7
Managing the clients file 6-9

APPENDIX A, Using /dev Entries A-1

APPENDIX B, Utilities B-1

APPENDIX C, Specifications C-1

APPENDIX D, Outbound Security D-1

APPENDIX E, Command Reference E-1

APPENDIX F, Dialnet Quick Start Guide F-1

APPENDIX G, Glossary G-1

Introduction CHAPTER 1

PortMaster Communications Servers are high-speed network access devices designed to operate in multi-protocol network environments. The hardware and software capabilities provide shared network access to printers, modems and other peripherals attached to the PortMaster; network access to terminals, X-terminals and remote users using dial-up internetworking. The PortMaster Communications Server provides the following features and capabilities:

- Expandable 10-to-30 port model (in 10 port increments)
- Compact 10 port only model
- Built-in SL/IP and PPP (interoperable with most implementations)
- Supports 115.2 Kb maximum data rate sustained on all 30 ports
- Multi-line load balancing for vastly increased performance
- Centronics compatible parallel printer port
- Thick, Thin, and Twisted Pair Ethernet ports
- Host Device Emulation
- On-line configuration
- Graphical administration software
- Advanced security (RADIUS, packet filtering, and dialback)
- Full network monitoring
- SNMP MIB-2 (Simple Network Management Protocol)
- Flash memory for better performance and easy upgrades
- Network Independent booting (local booting)

PortMaster operates as a smart communications device attached to an Ethernet network. It utilizes the TCP/IP and SPX/IPX networking protocols to communicate and establish virtual login and device services on host computers. Each of the ten to thirty PortMaster ports is independently configurable to support all types of RS-423 and RS-232 communications devices. The parallel port provides standard Centronics parallel communications for many printers.

Operating Modes

Advanced Dial-Up Internetworking

By using modems and standard telephone lines, local area networks can be economically and seamlessly connected. The PortMaster uses industry standard protocols (SLIP and PPP) to turn the PortMaster into a full multiprotocol router. This makes it compatible with all computers and networks which use the TCP/IP or SPX/IPX protocols. In addition, by incorporating an on-demand feature, dial-up telephone lines are only in use when there is data to be sent between networks. This reduces overall operating costs and increases the number of locations which can be tied together through a small number of modems.

Full Featured Remote Access

To support a growing number of telecommuters and field based portable computers requiring access to network resources such as file servers and printers, the PortMaster Communications Servers combine full-featured remote network access with comprehensive login security features like multi-level password protection automatic dial-back, TCP/IP packet filtering, and the RADIUS authentication service.

In addition, network users can gain access to external services through PortMaster managed modems. As a result, a small pool of modems can handle both dial-in and dial-out tasks which can reduce costs.

Cost-Effective Terminal Server

PortMaster Communications Servers offer a flexible low cost method of adding large numbers of terminals to computers. Each of the ports is independently configurable, and with host device emulation, you can easily configure a port to operate exactly like the built-in serial port of any workstation on the network. Each serial port can be configured to operate in four modes:

User Login Mode - Displays a user login prompt to establish a session on a host computer. In this mode, the PortMaster provides speed matching of one of three speeds from 300 through 115,200 baud.

Host Device Mode - Serial ports function as a UNIX tty device. The host accesses the port through a standard pseudo tty driver as if the port were physically connected as a hardware device. In addition ports can be accessed directly via available network services such as telnet.

Two Way Mode - In this mode, both User Login and Host Device Mode are supported. When a session has been established in user login mode, host device mode is suspended. When the host device is being directly accessed, user login mode is suspended. This allows for applications such as UUCP to utilize one modem in both directions.

Dialnet Mode - This mode allows the establishment of SLIP or PPP network connections over dedicated leased lines or over normal telephone lines using modems.

The ports can be configured in any number of the above combinations.

The parallel port, P0, functions in only the Host Device Mode.

Smart Features

The intelligence of the PortMaster allows it to be configured and monitored from a remote computer. By utilizing the a graphical user interface, all functions of PortMaster can be accessed with the click of a mouse. This includes installation, network setup, port configurations, and I/O monitoring. If a graphical display device is not available, all configuration parameters may also be set using a character mode terminal interface.

About This Manual

This manual is intended for use by those familiar with computers, Ethernet, TCP/IP, SPX/IPX and networking. Where needed, refer to your systems documentation for information on the various products. This manual is organized into six chapters:

Chapter 1: *Introduction* - describes the PortMaster hardware and software.

Chapter 2: *Installation* - describes the steps to follow to complete the installation of the PortMaster hardware and software.

Chapter 3: *Administration with X-Windows* - Describes the process of configuring the serial and parallel ports and the monitoring of PortMaster operations using the X-windows based PortMaster Console program.

Chapter 4: *Administration with an ASCII Terminal* - Describes the process for configuring the PortMaster and monitoring operations using the ASCII Terminal based PortMaster Console Program.

Chapter 5: *Administration with the Command Prompt Interface* - Describes the process used for configuring the PortMaster and monitoring operations from an ASCII terminal directly connected to a PortMaster serial port or from a telnet session.

Chapter 6: *RADIUS* - Describes the Remote Access Dial In User Service, an authentication protocol provided by Livingston at no additional charge.

Appendix A: *Using /dev Entries* - Describes Unix pseudo tty drivers and their use with the PortMaster.

Appendix B: *Utilities* - Describes local executables provided by Livingston for administration of the PortMaster from remote computers.

Appendix C: *Specifications* - Describes the hardware specifications of the PortMaster including electrical requirements.

Appendix D: *Outbound Port Security* - Describes the method of installing and maintaining secure outbound serial ports.

Appendix E: *Command Reference* - Lists all commands available from the Command Prompt Interface.

Appendix F: *Dialnet Quick Start Guide* - Checklist for three most common types of Dialnet connections.

Appendix G: *Glossary* - A Glossary of terms used in this manual and networking in general.

Index - Alphabetical reference for the entire manual.

New features in this release

- Support for routing Novell's IPX protocol
- IPX Packet Filtering
- SAP Service Filtering
- Enhanced diagnostic capability
- Extended debugging facilities
- Multiprotocol support for remote nodes and remote networks
- New Command mode features
- New Personal Computer based administration tools

Requesting Assistance

If you have any questions about the PortMaster, please use the following, toll-free number:

1-800-458-9966

Outside of the United States call:

510-426-0770

You may also send e-mail to:

support@livingston.com

Installation CHAPTER 2

This chapter describes installing the PortMaster hardware, the computer software, host installation and initializing the PortMaster.

Hardware Installation

The PortMaster can be situated sitting either right-side up or on either side. An optional rack-mount kit is available for easy installation into a rack unit. There are no internal adjustments or modifications for the user. You should locate the unit in a clean, cool environment, such as a normal office environment.

Rear Panel Layout of PortMaster PM-2

Figure 2-1 shows the locations of the major features of the PortMaster2 rear panel:

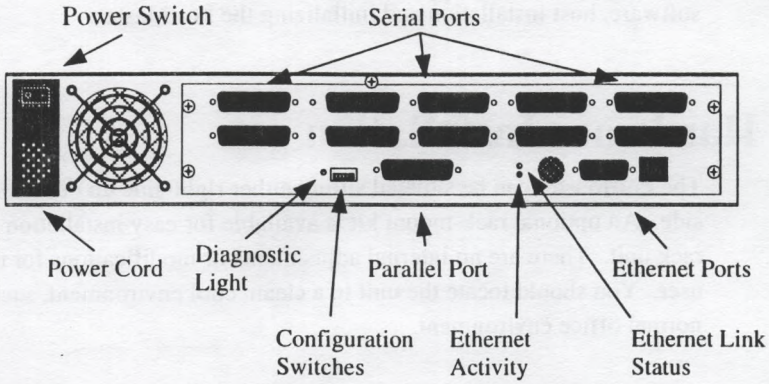


Figure 2-1. Rear Panel Layout PM-2

Rear Panel Layout of PortMaster 2e

The PortMaster PM-2 and PM-2E are functionally identical; the figure shown below is included for the purpose of orientation.

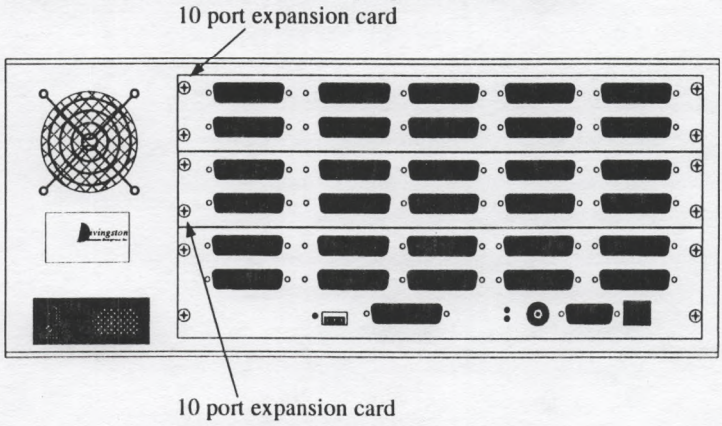


Figure 2-2. Rear Panel Layout 2e

Power - Power switch and power cord connector.

Serial Ports - Ten to thirty fully programmable RS-423 (RS-232 compatible) ports.

Parallel Port - A single Centronics compatible connector (P0)

Ethernet - There are three connectors: a BNC (round barrel) connector for use with Thin Net; a 15 pin AUI receptacle for Thick Ethernet or a compatible transceiver; a connector for twisted pair Ethernet (10BaseT). The active Ethernet interface is selected with the configuration switches on the rear of the PortMaster. These configuration settings are described in the next section "Configuration Switch Settings".

Diagnostic Light - This light provides diagnostic information about the status of the PortMaster. When power is first applied, the PortMaster performs a hardware self test. During this time, the diagnostic light will blink several times rapidly. After successfully completing the power on self test, the light will blink on and off once each second while loading the PortMaster operating system. When the PortMaster is fully operational the diagnostic light will remain on, and will blink off once every five seconds.

Ethernet Activity Light - This light blinks red whenever network traffic is detected.

Ethernet Link Status - When using Twisted Pair Ethernet (10BaseT) this light indicates the status of the link to the main hub.

Configuration Switches - These switches are used for Ethernet selection and diagnostic modes for the PortMaster. The following section describes the possible settings.

Configuration Switch Settings

There are five switches located next to the diagnostic light on the rear panel of the PortMaster. The switches are labeled with the numbers 1 through 5 (switch 1 is near the diagnostic light). All switches are set at the factory to the down position. These switches are used to set the ethernet configuration, examine self-test and diagnostic messages, and use network booting when necessary.

Self-Test and Diagnostic Messages - Booting the system with DIP switch 1 to the up position configures port S0 as the diagnostic console. During self-test and loading of the operating system, proper system operation can be verified by attaching a serial device (terminal or modem) to the S0 port at 9600 baud, 8 databits, 1 stopbit and no parity. Return switch 1 to the down position for normal operation.

Network Booting - Booting is normally performed from the FLASH Ram built into the PortMaster. Setting switch 2 to the up position allows Network Booting of the PortMaster.

Switch 3 is reserved for future use.

Ethernet Configuration - The ethernet configuration is determined by switches 4 and 5 according to the following table:

Switch Setting	**4**	**5**
Thin Net	Down	Down
Thick Net (AUI)	Down	Up
Twisted Pair (10BaseT)	Up	Up

Power Selection and Connection

AC power to the PortMaster is connected using a standard power cable. The PortMaster uses an auto-ranging power supply which allows it to automatically adjust to match the input voltage without setting a switch. The PortMaster will operate correctly at any AC voltage from 100V to 260V and frequencies from 50Hz to 60Hz.

To connect power to the PortMaster, connect the 3-conductor female plug to the rear panel of the PortMaster. Connect the 3-pin male plug to the appropriate source of AC power.

Serial Ports

There are 10 to 30 serial ports, S0 - S29. Each port utilizes a 25-pin D-type female connector. All standard RS-232 signals are available and the enhanced RS-423 standard is used. This allows for complete compatibility with RS-232 devices as well as RS-423 devices at higher data rates and over longer distances. The connection is configured as Data Terminal Equipment (DTE).

Parallel Port

There is one parallel printer output port: P0. This port utilizes a 25-pin D-type female connector. All standard Centronics signals are available.

Ethernet Connection

There are three types of Ethernet connection for the PortMaster:

Thin Ethernet - a BNC connector for direct connection to the computer's Thin Ethernet connector.

Thick Ethernet - the standard Ethernet D-type connector for connection to a transceiver on the Ethernet.

Twisted Pair Ethernet - a standard modular connector for direct connect to twisted pair hubs.

Which of these is in effect for your PortMaster is indicated by the switch settings on the rear of the PortMaster. Consult the section on configuring the switches for more information.

Connecting Serial Devices

To connect serial devices to the PortMaster, simply connect a male RS-232 connector to the appropriate rear panel connector (S0 through S9). Each of the serial ports is wired as Data Terminal Equipment (DTE). When connecting serial cables to these ports, secure the connectors together using either a screwdriver or the finger-screws mounted to the cable connector. Pin 1 is located in the upper-right corner of each connector (the row with the most pins).

The following table lists the PortMaster DTE serial port connections. The directions, input/output, are with respect to the PortMaster.

Pins not listed have no connection.

Connections for Serial Ports S0 - S29

Pin	Name	Description	
2	TXD	Transmit Data	(output)
3	RXD	Receive Data	(input)
4	RTS	Request To Send	(output)
5	CTS	Clear To Send	(input)
6	DSR	Data Set Ready	(input)
7	SGND	Signal Ground	
8	DCD	Data Carrier Detect	(input)
20	DTR	Data Terminal Ready	(output)

Connecting Parallel Devices

To connect a Centronics-compatible parallel device, use a cable that has a 25-pin male DB-25 connector at one end and a 36-pin Centronics connector at the opposite end. The P0 pinout is compatible with the parallel ports of Personal Computers. When connecting the parallel cable to this port, secure the connectors together using a screwdriver or the finger-screws mounted to the cable connector.

Pin 1 is located in the upper-right corner of the rear panel connector (the row with the most pins). The following table lists the pin out of the Parallel Port.

Connections for Parallel Port - P0

Pin	Name	Description	
1	Strobe	Strobe	(output)
2	D0	Data Bit 0	
3	D1	Data Bit 1	
4	D2	Data Bit 2	
5	D3	Data Bit 3	
6	D4	Data Bit 4	
7	D5	Data Bit 5	
8	D6	Data Bit 6	
9	D7	Data Bit 7	
10	ACK	Acknowledge	(input)
11	BUSY	Printer Busy	(input)
12	PE	Paper Empty	(input)
13	Sel.	Device Select	(output)
14	AF	Auto Feed	(output)
15	Err.	Error	(output)
16	Init.	Initialize Printer	(output)
17	Sel In.	Select Input	(output)
18-25	GND	Ground Connections	

Connecting the Ethernet

The PortMaster provides connectors for Thin, Twisted Pair, or Thick Ethernet.

Thin Ethernet

The Thin Ethernet BNC connector is the round connector on the left of the 15-pin AUI connector. Connect a coaxial cable between the PortMaster Thin Ethernet connector and the network or Unix workstation. Termination is required at each end of the Thin Ethernet coaxial cable. Use the BNC T-adapter included with the PortMaster. Figure 2-2 illustrates a Thin Ethernet connection between the PortMaster and a workstation.

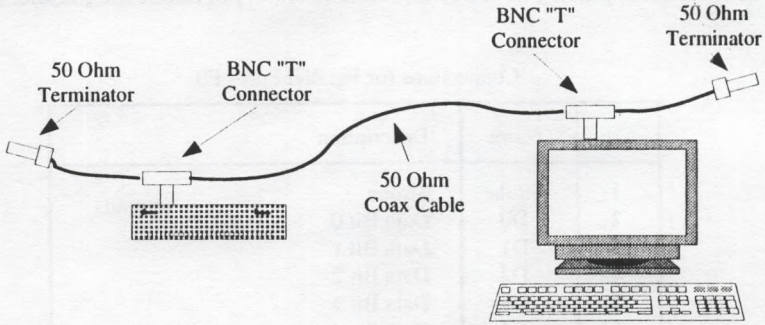


Figure 2-2. Thin Ethernet Connection

Thick Ethernet

A 15 Pin D-type connector is located on the rear panel of the PortMaster to the right of the Thin Ethernet BNC connector. Connect the Ethernet transceiver cable to the PortMaster rear panel connector. Slide the locking ring until the connection is secure.

Twisted Pair Ethernet

A modular connector for use with Twisted Pair Ethernet is located to the right of the 15-pin AUI connector. This connector should be attached via standard Twisted Pair wiring to a hub unit which supports the 10BaseT standard.

Workstation Software Installation

PortMaster installation software is available in several forms of media and for a variety of computer platforms. Consult the Livingston Price List for the correct software for your system.

This software is not required when using the PortMaster. However, it does provide two valuable functions:

Administration - The **pmconsole** administration software provides a user friendly interface for configuring and monitoring the PortMaster.

Host Device Emulation - This software (which is installed on your computer) allows the serial ports on the PortMaster to be used as built-in serial and parallel ports for your computer. This allows software applications which access host-resident ports to operate unmodified with the PortMaster.

To install the software you will need approximately 3 MB of disk space available.

Loading from Tape or Floppy Diskette

This procedure describes the installation of the PortMaster software on UNIX computer systems:

- Login as root.
- Using mkdir, create a directory called /usr/portmaster. This is the recommended directory location and name. If you wish to use a different directory, substitute that name in the following command:

  mkdir /usr/portmaster

- Change your working directory to /usr/portmaster.

  cd /usr/portmaster

Note: *It is a good idea to place the portmaster directory in your $path environment ($PATH for Bourne and Korn Shells), this will allow you to run the various executables without specifying the full path.*

- Load the diskette or tape into the appropriate drive.
- Type the command:

  tar xvf /dev/<device>

Where <device> is the raw device of your tape or diskette drive. Consult your computer system documentation for the correct device name. For example, to load the information from a Sun Microsystems SCSI tape drive, you would type the command:

tar xvf /dev/rst0

While the software is being extracted from the tape or diskette, the list of files being extracted will be displayed. After the software has been fully extracted, go on to "Running **pminstall**".

Running pminstall

At this point in the installation procedure you should be logged on as root and have the /usr/portmaster directory as your current working directory. Simply enter the command:

pminstall

After decompressing the PortMaster distribution files, your display should show the following menu:

```
1 Portmaster Internet Address Setup
2 Host Installation
3 Portmaster Upgrade
4 Host Upgrade
5 Exit

Please select an option from above:
```

Use this menu to select the appropriate option. The following paragraphs describe the functions of the first two menu selections.

Host Software Installation

The first time you load the host software, select Item 2 from the menu, "Host Installation". If you are adding another PortMaster to the network, go on to the following section **PortMaster Internet Address Setup**. From the **pminstall** menu, select 2, followed by RETURN. The following dialog will be displayed:

[Note: *The contents of the following dialog will vary depending on the extent to which networking functions have already been installed on your UNIX Workstation. If this is a stand-alone workstation which has never been connected to a network, a simple "y" (yes) response to all questions will work well. If this workstation is connected to an existing network please consult your network administrator and network administration manuals for the correct responses.]*

```
Performing Host Installation.

Default Host internet address = 192.9.200.1
Use default? (y/n) y
Adding host entry in /etc/hosts for <host>
Starting local network interface.
Performing Software Installation.
Updating /etc/services
Installing in.pmd daemon
Updating /etc/inetd.conf
Host Installation Completed.

1 Portmaster Internet Address Setup
2 Host Installation
3 Portmaster Upgrade
4 Host Upgrade
5 Exit

Please select an option from above:
```

The menu is then redisplayed. At this point, the host software is installed and the host internet address has been assigned.

PortMaster Internet Address Setup

Verify that the new PortMaster has been physically connected to the network and has been powered on before starting this section.

From the **pminstall** menu, select item 1, follow by RETURN. The following dialog will be displayed:

```
Please enter the PortMaster name:<portmaster_name>
```

Where *<portmaster_name>* is the "network" name you want to assign to the new PortMaster. If the PortMaster and UNIX Workstation are being installed on a stand-alone network then any name may be used. If this name has not already been established as a valid network host name, you will receive the following prompt:

```
Cannot find host entry for <portmaster_name>

Would you like to add a new one? (y/n) y
Use system assigned internet address? (y/n) y
Confirm add: Host: <portmaster_name> Address: 192.9.200.2 ?
(y/n) y
```

Once the PortMaster name and internet address have been verified, the following messages will appear (this may take between 5 and 20 seconds):

```
Listening on network for heartbeat of new PortMaster ...

Found heartbeat
PortMaster internet notification complete.
```

[Note: *If an error message is displayed during this step indicating a failure to open any network devices, verify all networking resources are installed in your UNIX kernel. On Sun Workstations, the pseudo devices: snit, pf, nbuf, and clone must be installed. These service names will differ from system to system. Refer to your Workstation installation documentation for more complete descriptions.]*

When the Portmaster Internet Address Setup has completed, the main installation menu will be displayed.

```
1 Portmaster Internet Address Setup
2 Host Installation
3 Portmaster Upgrade
4 Host Upgrade
5 Exit

Please select an option from above: 5
```

At this point, the new PortMaster is initialized and known to the network. The next chapter, Administration, describes the administration of the PortMaster, port configurations, etc. Read the section on logging into the PortMaster and then complete the steps described in setting the Global Configuration.

Note: If the above procedure fails, and you get the error message:

```
PortMaster internet address setup is not supported on this
system.  Follow instructions for setting the PortMaster IP
Address using the Command line interface in the PortMaster
User's Manual.
```

1- Edit the /etc/hosts file. Add an entry for the new PortMaster.

For example:

#

Livingston Enterprises PortMasters

#

192.9.200.8 portmaster1

The IP address assigned to the PortMaster and the PortMaster name should be replaced with the locally assigned designations in the example above.

2- Connect a terminal to any serial port of the new PortMaster with a null modem cable (pins 2 and 3 interchanged). Set the communication parameters on the terminal to the following:

9600 baud

8 databits

1 stop bit

no parity

A login prompt should be displayed on the terminal screen. At the login prompt enter:

login: **!root**

The PortMaster will request that you enter a password. Since no password has been entered and stored in a new PortMaster, just press the *Return* key.

The Command prompt should now be displayed. Enter the following command to set the IP address of the new PortMaster (the locally assigned address as entered in the /etc/hosts table should be substituted for the example shown below):

Command> **set address 192.9.200.8**

A confirmation message should be displayed indicating the address change. Next save the address in the PortMaster memory by entering the following command:

Command> **save all**

Exit the command mode by entering the folowing command:

Command> **quit**

Remove the terminal and proceed as described in this chapter.

Administration CHAPTER 3

PortMaster Console

PortMaster Console (**pmconsole**) is the PortMaster administration program. **pmconsole** is used to administer the Livingston Enterprises Communications Servers and Internetwork Routers. The PortMaster can be configured using one of three user interfaces: X-Windows, a full screen ASCII terminal interface, or the Command Prompt interface. The graphical interface provides several windows through which you can configure the PortMaster ports, monitor the performance, and install other PortMasters on your network. The terminal interface is described in Chapter 4, and the Command Processor interface is described in Chapter 5.

Running pmconsole

To run the **pmconsole** program, enter the following command:

pmconsole *[-o | -t] [-n]*

If no options are specified, **pmconsole** will automatically use the interface which best matches your current environment (for example, if you are running X-windows and your DISPLAY variable is set, it will use the graphical interface). If you wish to specify a particular user interface the optional arguments are:

-o - Use the X-windows based User Interface.

-t - Use the ASCII Terminal User Interface.

In normal operation, **pmconsole** will automatically translate all IP addresses into host names as defined in your systems hosts database. The **-n** option causes the display of only numeric IP addresses.

pmconsole with X-Windows

The X-Windows graphical interface provides several windows to configure the PortMaster ports, monitor performance, and install other PortMasters. This can be run from any X-windows compatible device.

Each window in the PortMaster Console has a set of buttons. Items with triangles have menus which can be seen by pressing the right mouse button. Other items can be selected by pressing the left mouse button.

When **pmconsole** is started, the window in Figure 3-1 will be displayed.

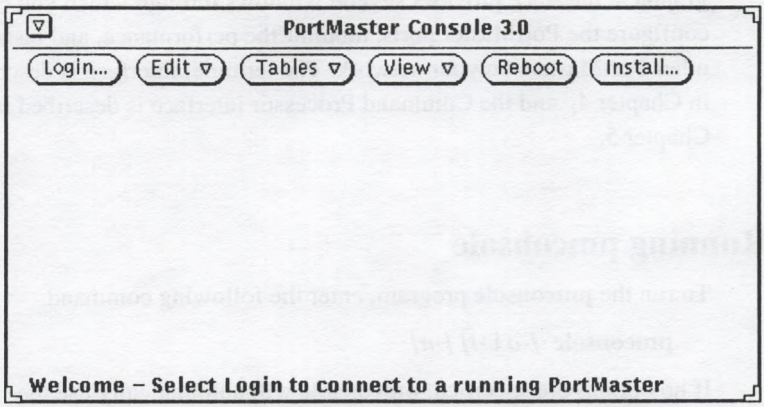


Figure 3-1. PortMaster Console login display

This is the primary window of the PortMaster Console program. From this window all other windows and functions of the software are accessible. The buttons across the top of the window are used to access the various functions. The PortMaster Console window has the following buttons:

- **Login** - to access any PortMaster
- **Edit** - to edit (change) port configurations, network configurations, administration passwords, SNMP and RADIUS.
- **Tables** - to view and edit Dial-out Locations, User Entries, the Hosts

Table, the Static Routing Table or the Packet Filters Table.

- **View** - to view port configurations, data traffic, and established dial-out connections.
- **Reboot** - to reboot the PortMaster
- **Install** - to install a PortMaster onto the network or to install new software releases.

A detailed description of each of these button functions follows.

PortMaster Login

To communicate with any PortMaster which has already been installed onto the network use the **Login** function. This function establishes a link with the PortMaster and allows you to utilize all other functions. To Login, use the following steps:

1. Place the mouse pointer on the **Login** button and click the left mouse button.

2. The Password Window will be displayed. Enter the PortMaster name assigned during the installation procedure, then press <RETURN>.

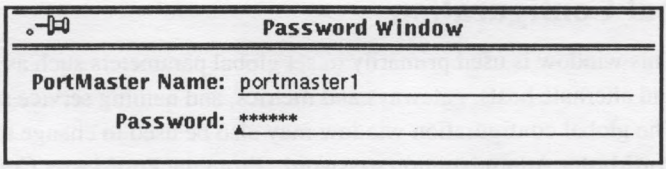


Figure 3-2. PortMaster Password Window

3. Enter the password, if any, and press <RETURN>. When the PortMaster is shipped from the factory there is no password. There will be a message stating that the connection is being attempted. With a successful connection, the main PortMaster window (Figure 3-3) will be displayed.

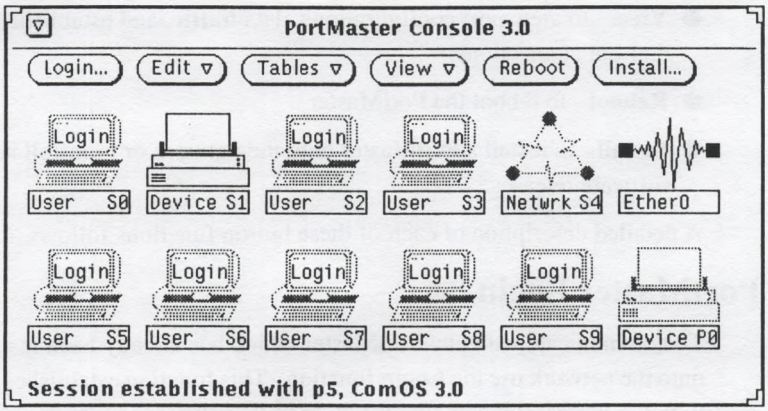


Figure 3-3. PortMaster Console icon window

The PortMaster Console window displays the port icons for the serial ports, the parallel port, and for the ethernet port. In addition other configuration items can be edited through the menu's provided by the Edit and Tables buttons.

Global Configuration

This window is used primarily to set global parameters such as default and alternate hosts, gateways and metrics, and naming service selection. The global configuration window may also be used to change the PortMaster Administration password. From the PortMaster Console, do the following:

1. Position the mouse pointer on the **Edit** button and press the right mouse button. The **Edit Menu** will appear.

2. Select **Global**. The window in Figure 3-4 will be displayed.

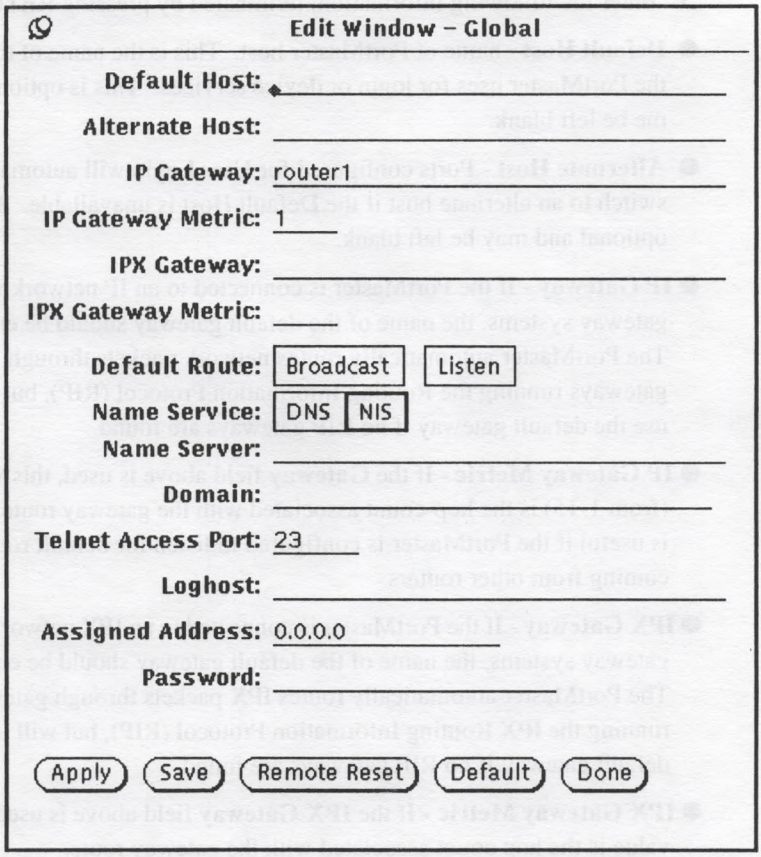


Figure 3-4. Edit Window - Global

The Global Window has the following buttons:

- **APPLY** - send the configuration to PortMaster memory.
- **SAVE** - stores the port configuration in the PortMaster Flash RAM.
- **REMOTE RESET** - reset the PortMaster parallel and serial port(s) using the values stored by the **APPLY** or **SAVE** selection.
- **DEFAULT** - set the *on-screen* values to the default configuration.
- **DONE** - return to the PortMaster Console window.

3. Enter the following information, terminated by pressing RETURN:

- **Default Host** - name of PortMaster host. This is the name of the host the PortMaster uses for login or device services. This is optional and me be left blank.
- **Alternate Host** - Ports configured for User Login will automatically switch to an alternate host if the Default Host is unavailable. This is optional and may be left blank.
- **IP Gateway** - If the PortMaster is connected to an IP network with gateway systems, the name of the default gateway should be entered. The PortMaster automatically routes network packets through gateways running the Routing Information Protocol (RIP), but will use the default gateway if no RIP gateways are found.
- **IP Gateway Metric** - If the **Gateway** field above is used, this value (from 1-15) is the hop-count associated with the gateway route. This is useful if the PortMaster is configured to listen for default routes coming from other routers.
- **IPX Gateway** - If the PortMaster is connected to an IPX network with gateway systems, the name of the default gateway should be entered. The PortMaster automatically routes IPX packets through gateways running the IPX Routing Information Protocol (RIP), but will use the default gateway if no RIP gateways are found.
- **IPX Gateway Metric** - If the **IPX Gateway** field above is used, this value is the hop count associated with the gateway route.
- **Default Route** - Any combination of "Broadcast" and "Listen" can be used. If "Broadcast" is selected, the PortMaster will send default route information as part of its normal RIP messages. If "Listen" is selected, the PortMaster will accept default route information from other routers connected to any of the interfaces. The default is to not Broadcast or Listen. If selected, defaults routes are broadcast or listened to across all interfaces, including serial interfaces configured for PPP or SL/IP.
- **Name Service** - For networks which use the Network Information

Service (NIS), also known as YP, the PortMaster can be configured to use this service for host name matching. Select DNS if your network uses the Domain Name Service.

- **Name Server** - Enter the name of the server providing the name service selected.
- **Domain** - if DNS or NIS is used, the domain name must be entered.
- **Telnet Access Port** - The PortMaster allows the system administrator to access all of the PortMaster administration functions through a command line interface. These functions can be reached by logging onto the PortMaster with a telnet session. This field identifies the specific TCP port number for the PortMaster to listen on for incoming telnet administration sessions. The default value is "23". Any number from 0 to 65536 may be used. Ports numbered from 10000 through 10100 are reserved for an internal filter used for outbound security. See Appendix E, "Outbound Security" for more information. If 0 is selected, the PortMaster will disable the telnet administration function.
- **Loghost** - The PortMaster supports "syslog" network accounting. If a host is entered in this field, the PortMaster will log authentication information to this host using the system facility "auth" and the priority of "info" (auth.info). Consult your system's syslogd and /etc/syslog.conf manual pages for more information on this service.
- **Assigned Address** - This field is used in conjunction with Dialnet. It is only used for network login users using the PPP or SL/IP protocols who are being assigned a temporary address for their active session. If a network user in the Users Table has been set to use an "Assigned Address", the PortMaster must allocate a temporary IP address to be used for their active session. This IP address is retrieved from a pool of addresses maintained by the PortMaster. The IP address entered in this field will be used as the first free address in the pool of addresses. The PortMaster will allocate as many addresses as there are ports configured for Dialnet access.
- **Password** - PortMaster administration password. The password entry

must be entered twice to ensure that the password was entered correctly.

Be sure to press < RETURN > after each entry.

The password can be changed at any time by following the procedures in this section.

4. Select the **SAVE** button to store the data in the PortMaster. At the bottom of the window will be a message:

Configuration successfully saved.

5. Select the **DONE** button.

Ethernet Port Configuration

To configure the ethernet port, use the following procedure:

1. From the PortMaster Console, select the ethernet port by placing the mouse pointer on the **Ether0** icon and clicking the left mouse button.

2. Select the **Edit** button. The **Edit Window** for the ethernet port (Figure 3-5) will appear. From this window you can modify the ethernet port configuration parameters.

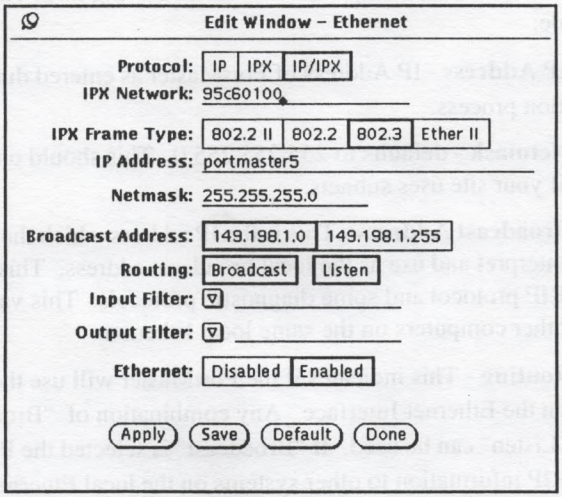


Figure 3-5. Edit Window - Ethernet Port

The **Edit Window - Ethernet** has the following buttons:

- **APPLY** - send the configuration to PortMaster memory.
- **SAVE** - performs an **APPLY** and stores the port configuration in the PortMaster non-volatile storage (FLASH RAM).
- **DEFAULT** - set the *on-screen* values to the default configuration.
- **DONE** - return to the PortMaster Console window.

3. Enter the following information, terminated by pressing RETURN:

- **Protocol** - select one of IP, IPX, or IP and IPX.

If IPX or IP/IPX is selected, you must fill in the following two entries:

- **IPX Network** - enter the address of your IPX network.
- **IPX Frame Type** - specify the ethernet frame type. This should be set to match your Novell file server settings.

If you have selected IP or IP/IPX the following three entries must be made:

- **IP Address** - IP Address of PortMaster as entered during the installation process.
- **Netmask** - defaults to 255.255.255.0. This should only be modified if your site uses subnets.
- **Broadcast Address** - This is the IP address which the PortMaster will interpret and use as the local broadcast address. This is used by the RIP protocol and some diagnostic protocols. This value *must* match other computers on the same local Ethernet.
- **Routing** - This indicates if the PortMaster will use the RIP protocol on the Ethernet Interface. Any combination of "Broadcast" or "Listen" can be used. If "Broadcast" is selected the PortMaster sends RIP information to other systems on the local Ethernet. If "Listen" is selected, the PortMaster accepts RIP information from other routers on the local Ethernet. The default is to both Broadcast and Listen.
- **Input Filter** - Allows you to select from a list of all available input filters on the PortMaster. When specified, all packets received from the Ethernet interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Packet Filters" toward the end of this chapter.
- **Output Filter** - Allows you to select from a list of all available output filters on the PortMaster. When specified, all packets being sent to the Ethernet interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Packet Filters" later in this chapter.
- **Ethernet** - This field enables IP traffic on the Ethernet interface of the PortMaster. If set to disable, no IP packets are sent or received on this interface. It should only be disabled when the PortMaster is not being attached directly to the local Ethernet.

Installation from PortMaster Console

To install or upgrade a PortMaster from the PortMaster Console, instead of using the program **pminstall** as described in Chapter 2, select the **INSTALL** button. The window in Figure 3-6 will appear. The option buttons in this window are the same options available with **pminstall** (See Chapter 2, *Running **pminstall***).

- **New PortMaster**
- **New Host**
- **Upgrade PortMaster**
- **Upgrade Host.**
- **Done**.

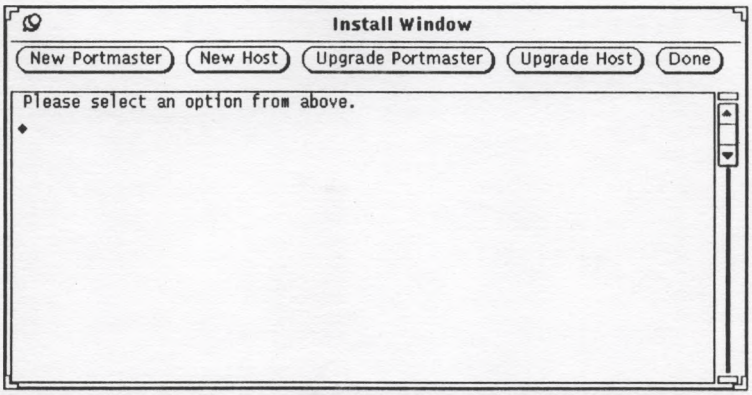


Figure 3-6. PortMaster Install window

One reason for using this method instead of running **pminstall** from the UNIX command line is that the workstation window can be scrolled. In this way you can view the entire setup process by using the scroll bars. The Upgrade PortMaster button is used for the installation of new software releases.

Serial Port Configuration

To set the configuration of any of the serial ports, use the following procedure:

1. From the PortMaster Console window, select a serial port icon by placing the mouse pointer on the icon of the port and clicking the left mouse button.

2. Select the Edit button. The Edit Window for the selected serial port (Figure 3-7) will appear. From this window you can modify the serial port configuration parameters.

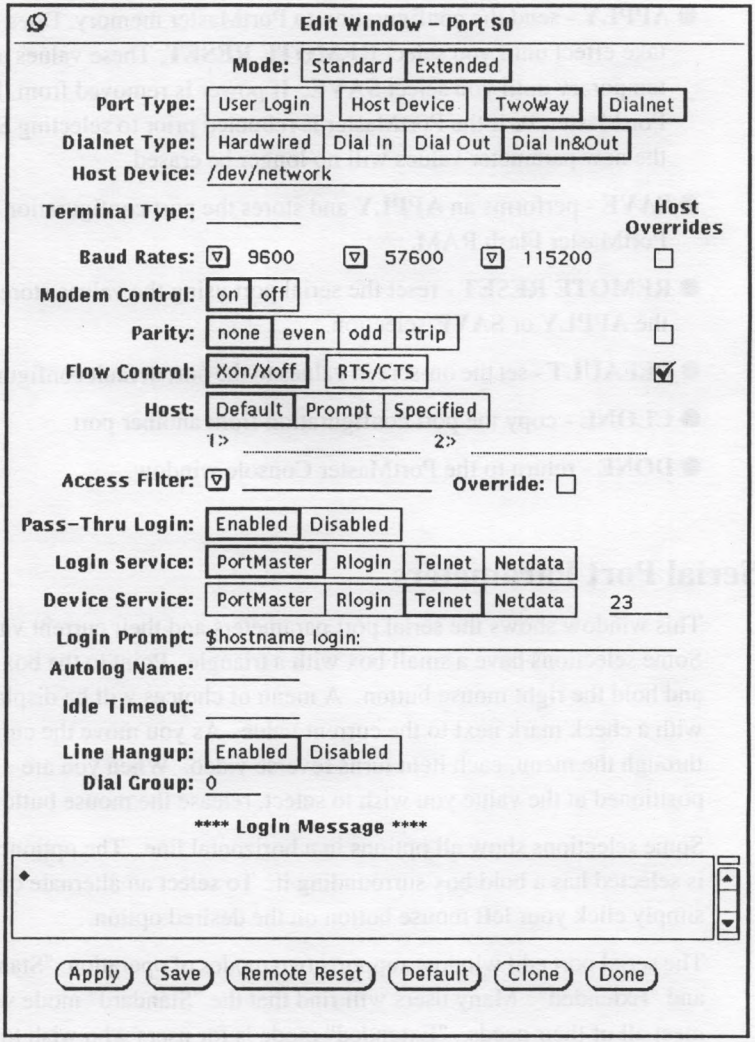

Edit Window – Port S0
Mode: Standard Extended
Port Type: User Login Host Device TwoWay Dialnet
Dialnet Type: Hardwired Dial In Dial Out Dial In&Out
Host Device: /dev/network
Terminal Type:
Host Overrides
Baud Rates: 9600 57600 115200
Modem Control: on off
Parity: none even odd strip
Flow Control: Xon/Xoff RTS/CTS
Host: Default Prompt Specified
1> 2>
Access Filter: Override:
Pass-Thru Login: Enabled Disabled
Login Service: PortMaster Rlogin Telnet Netdata
Device Service: PortMaster Rlogin Telnet Netdata 23
Login Prompt: $hostname login:
Autolog Name:
Idle Timeout:
Line Hangup: Enabled Disabled
Dial Group: 0
**** Login Message ****
Apply Save Remote Reset Default Clone Done

Figure 3-7. Edit Window - Serial Port

The Edit Window has the following buttons:

- **APPLY** - send the configuration to PortMaster memory. Does not take effect until you select **REMOTE RESET**. These values are temporary until you select **SAVE**. If power is removed from the PortMaster, or if the PortMaster is rebooted prior to selecting **SAVE**, the new parameter values will no longer be erased.
- **SAVE** - performs an **APPLY** and stores the port configuration in the PortMaster Flash RAM.
- **REMOTE RESET** - reset the serial port using the values stored by the **APPLY** or **SAVE** selection.
- **DEFAULT** - set the on-screen values to the port default configuration.
- **CLONE** - copy the port configuration from another port.
- **DONE** - return to the PortMaster Console window.

Serial Port Parameters

This window shows the serial port parameters and their current values. Some selections have a small box with a triangle. Point to the box, click and hold the right mouse button. A menu of choices will be displayed, with a check mark next to the current value. As you move the cursor through the menu, each item turns reverse video. When you are positioned at the value you wish to select, release the mouse button.

Some selections show all options in a horizontal line. The option which is selected has a bold box surrounding it. To select an alternate option, simply click your left mouse button on the desired option.

The serial port edit window supports two modes of operation: "Standard" and "Extended". Many users will find that the "Standard" mode will meet all of their needs. "Extended" mode is for users who wish to customize the operation of the serial port.

Standard Mode Parameters

Port Type

User Login - The specified port will display a login prompt to the user. After successful baud rate matching and receiving a login name, the user will either be authenticated from the PortMaster Users Table, the RADIUS Authentication Server, or will be transferred directly to a login session on the host computer as specified for that port.

Host Device - The port operates as a host controlled device on the host workstation or as a network accessible device using telnet, rlogin, or a binary TCP connection (See "Device Service" in Extended Mode Parameters later in this chapter). The Host Device field described below must be entered.

Two-Way - The port will operate in User Login mode if carrier is detected on pin 8 of the RS-232 connector. Otherwise it can be accessed as a host device. The Host Device field described below must be entered.

Dialnet - This option can be selected with the other Port Types if the "**Dialnet Type**" field is set to a value other than "**Hardwired**". The port becomes available for running the Serial Line Internet Protocol (SLIP) or the Point to Point Protocol (PPP) for establishing connections between remote sites via modem. The specific services are defined in the following "Dialnet Type" fields.

Dialnet Type

Hardwired - The port is being used for a dedicated network connection between two sites. No modem dialing or authentication is required. The port immediately begins running the specified protocol. In this mode, none of the other port types can be used with Dialnet.

Dial In - In this mode, the port will accept dial-in only network connections. The remote system (or user) will be required to enter a user name and password. Dial-In network connections are controlled by the User Table described later in this chapter.

Dial Out - In this mode, the port becomes available for dialing to remote

destinations and initiating network connections to those destinations. Dial Out network connections are controlled by the **Location Table** described later in this chapter.

Dial In & Out - In this mode, the port will accept dial-in network connections, as well as being available for dial out to remote destinations. In any of the three Dial modes, the port can also be configured to support other port operations concurrently. If one of the other port types is selected, that port type and **Dialnet** will be highlighted. If one of the other port types is selected, those port type parameters become available.

Host Device

This field will be displayed in either the **Host Device** or **Two-Way** modes when using the **PortMaster** device service. The Host Device name is the name of a pseudo tty device in the host /dev directory.

Standard device entries are:

/dev/ttyp0 through /dev/ttypf
/dev/ttyq0 through /dev/ttyqf
/dev/ttyr0 through /dev/ttyrf

Since other programs on the host use these same pseudo tty devices, care should be taken in selecting the devices for the PortMaster. Since most dynamically allocated devices are taken from the beginning of the list, it is recommended that devices at the end of the list be used for the PortMaster. Refer to Appendix A for discussion of device drivers.

When using the port as a network accessible device using rlogin, telnet, or netdata, this entry should be set to "/dev/network".

Terminal Type

This optional field will be displayed in either **User Login** or **Two-Way** modes. When a new session is established on the host workstation, this terminal type will be set in the user's environment. A valid entry from the host's termcap or terminfo database must be entered. If this field is left blank, the host assumes a "dumb" terminal.

Baud Rates

Three different baud rates may be specified. These baud rates are used for speed matching with the device being attached to the PortMaster. Speeds are sequentially matched from the first baud rate (left side) through the third baud rate (right side). In **Host Device** mode, only the first baud rate is used. With newer modems and terminals the baud rate should be set to always run at a fixed data rate. This is done by setting all three baud rates to the same value.

- First baud - the first baud rate that PortMaster uses to synchronize with the attached device. Speeds from 300 bps to 115.2 Kbps are available (the default is 9600 bps).
- Second baud - a second baud rate that PortMaster can use to synchronize with the attached device. Data rates from 300 bps to 115.2 Kbps are available (the default is 9600 bps).
- Third baud - a third baud rate that PortMaster can use to synchronize with the attached device. Data rates from 300 bps to 115.2 Kbps are available (the default is 9600 bps).

Modem Control

On or off may be selected. The default is "off". If "on" is selected, the PortMaster uses the modem carrier detect line. The device will be idle until the carrier detect line is asserted. This value should be set to "on" when a modem has been attached. In addition, the modem should be set for "Normal" carrier detect.

Parity

Even, odd, none, or strip may be selected. The default is "none". This value should be set to match the device attached to the PortMaster. When even or odd is selected, 7 databits and 1 stop bit are assumed. When none or strip is selected, 8 databits and 1 stop bit are assumed. When strip is selected, the parity bit will be removed from the data as it is received by the PortMaster. See the "Extended Mode Parameters" section if another combination is required.

Login Message

This is a message displayed to the user prior to login; the message may be up to 240 characters in length.

Extended Mode Parameters

In addition to the parameters described above in "Standard Mode Parameters", the following parameters may be set when Extended Mode is selected.

Flow Control

The PortMaster supports two types of flow control:

Xon/Xoff - This is a software flow control which is supported by most devices. By using ASCII control characters DC1 and DC3 the PortMaster communicates with the attached device to start and stop the flow of data.

RTS/CTS - This is for devices where hardware flow control is required. When the PortMaster is able to receive data from the attached device, it raises Request to Send (RTS) on pin 4 of the RS-232 connector. Output from the PortMaster will only occur if the Clear to Send (CTS) modem line on pin 5 of the RS-232 connector is raised by the attached device.

Host

The port can be configured to support three different ways of determining the Host to establish a login session on:

Default - In this mode, the host entries entered in the global (network) edit screen are used for this port.

Prompt - In this mode, the user is given a host prompt (before the standard login prompt). The user then is required to enter a valid host name or internet address for a host on the network.

Specified - In this mode a primary host and up to three alternate hosts may be entered for this specific port. In this way each port can be independently assigned to a specific network host. When this option is selected, the additional fields will appear on the display for the entry of

the host names.

Access Filter

An optional access control filter can be specified for the port. This filter is taken from the standard packet filter table described later in this chapter. After the user specifies a host, its address is compared against the designated filter. If the address is "permitted" by the filter, the user's connection will be allowed. If not, access will be denied. If the Access Override field is checked, and access has been denied, the user will be prompted for a username and password. The user's access filter from the Users Table will then be used to determine if the user's private access filter provides sufficient additional capability to allow access to the designated host.

Login Service

The port can be configured to use one of four different network services for establishing login sessions.

PortMaster - This is the default service and can be used with any host workstation which has had a "Host Installation" performed from either **pminstall** or the install window of **pmconsole**. This is the preferred service because it makes the port operate like the serial ports physically installed in the host. In addition it is the most efficient and highest performance service available.

Rlogin - This service is generally supported by a large number of mixed UNIX based computers. Therefore, where it is impractical to utilize the PortMaster service, Rlogin should be selected.

Telnet - This service is generally supported by most TCP/IP computers. Therefore, in a network where mixed hardware and operating systems will be used by this port, Telnet should be selected. The default TCP port number for telnet is 23, however an additional data entry field is provided to enter an alternate TCP port if required.

Netdata - This service can be used to create a virtual connection between the port and another serial port on a different PortMaster or for allowing clear channel TCP network connections from other hosts on the

network. The default TCP port number for netdata is 6000, however an additional data entry field is provided to enter an alternate TCP port if required. If using the virtual connection service, the serial port on the remote PortMaster must be configured as a Host Device Port using the same service and TCP port number.

Device Service

The port can be configured to use one of four different network device services.

PortMaster - This is the default service and can be used with any host workstation which has had a "Host Installation" performed from either **pminstall** or the install window of **pmconsole**. This is the preferred service because it makes the port operate like the serial ports physically installed in the workstation. When selected, the port is accessed through a /dev/tty device on the host workstation.

Rlogin - This service is generally supported by a large number of mixed UNIX based computers. Therefore, this service can be utilized to allow UNIX based workstations on the network to initiate an rlogin session to the PortMaster. Once the session is successfully established, the host application will be able to directly read and write data to the serial port. If multiple ports on the PortMaster are configured to use this service it will automatically create a "pool" of ports which can be accessed by other hosts. When all ports are in use, new users will be given a "Connection Refused" message.

Telnet - This service is generally supported by most TCP/IP computers. Therefore, this service allows many different types of computers on the network to initiate a telnet session to the PortMaster. Once the session is successfully established, the host application will be able to directly read and write data to the serial port. If multiple ports on the PortMaster are configured to use this service it will automatically create a "pool" of ports which can be accessed by other hosts. When all ports are in use, new users will be given a "Connection Refused" indication. The default TCP port number for telnet is 23. An additional data entry field is provided to enter an alternate TCP port if required.

Netdata - This service can be used for customized application programs that need a TCP connection directly to a serial port on the PortMaster. Programs which use the "socket" interface (or a similar TCP interface) are provided with a direct data link to the PortMaster serial port. Port operating parameters are set with **pmconsole**. The application can then open the socket connection and immediately begin reading and writing data to the PortMaster. No special option negotiation or protocol is required. The default TCP port number for netdata is 6000, however an additional data entry field is provided to enter an alternate TCP port if required. If multiple ports on the PortMaster are configured to use this service with the same TCP port number, it will automatically create a "pool" of ports which can be accessed by other hosts. When all ports are in use, new users will be given a "Connection Refused" message.

Login Prompt

This field allows the administrator to customize the login prompt the user will see. Any ASCII characters may be entered. The default is to display the active host name followed be the word "login:". If the string "$hostname" is included in the login prompt, the active host name is substituted for the string.

Autolog Name

If this field is filled in, the user will not receive the standard login prompt. Instead, the PortMaster will automatically initiate a session on the host system as if the user had typed the **Autolog Name** in response to the login prompt.

Idle Timeout

The idle timeout specifies how long the PortMaster should wait after the activity on the port stops before disconnecting the session. The Idle timeout is specified in minutes and can be any value from 0 to 240. If set to 0, the idle timer will be disabled.

Line Hangup

If this field is enabled, the DTR signal in the RS-232 connector will be

momentarily dropped to cause a modem or similar device to hangup after the termination of a user session. If disabled, DTR will not drop after the session terminates.

Pass-Thru Login

If this field is enabled, user's whose names do not match the local PortMaster users table will automatically be forwarded to the host specified in the "Host" field above. If this field is disabled, only users who are in the local user file or authenticated by RADIUS will be able to logon.

Dial Group

The Dial Group is used to assign serial ports to modem pools or groups. When the PortMaster initiates a dial-out connection to a remote site, it will only allocate a port from the dial group that has been specified for that location in the Location Table. Valid dial groups are numbered from 0 to 99. The default is 0.

Host Overrides

The PortMaster allows host overrides to be selected for Baud Rate, Parity, Databits, and Flow Control. This feature allows the host to alter the active parameters via software control (i.e., system ioctl calls). Parameters which have a check mark in the box opposite them can be overridden. The default is that the Host can only turn Xon/Xoff flow control on and off. This is useful for many UNIX utilities like uucp and tip. If the parameter is not checked it cannot be overridden. In this case system requests to change these parameters will be ignored.

Hardwired Dialnet parameters

By selecting "Dialnet" in conjunction with "Hardwired" the following window will be displayed:

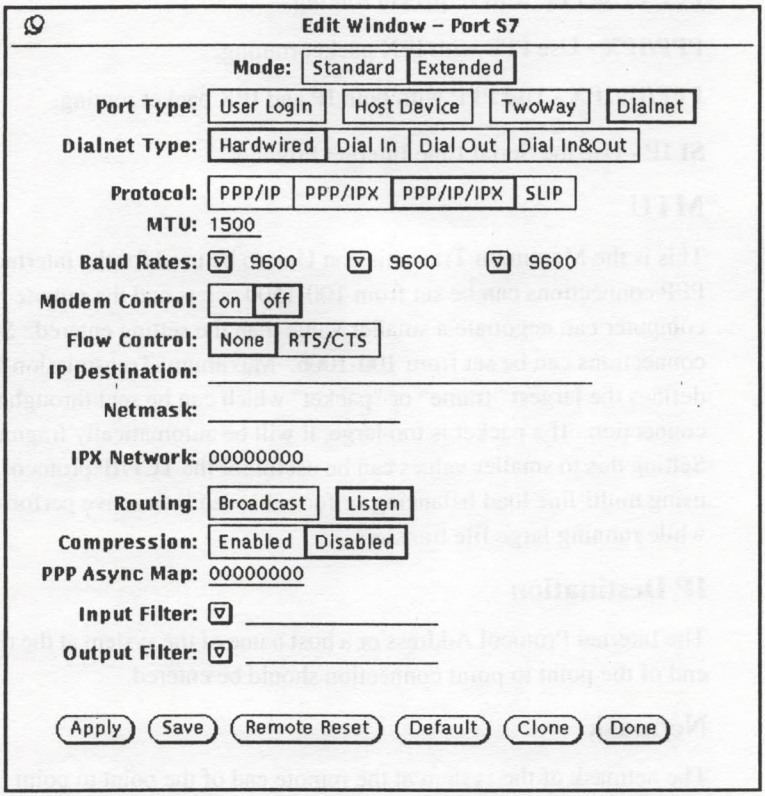

Edit Window – Port S7
Mode: Standard Extended
Port Type: User Login Host Device TwoWay Dialnet
Dialnet Type: Hardwired Dial In Dial Out Dial In&Out
Protocol: PPP/IP PPP/IPX PPP/IP/IPX SLIP
MTU: 1500
Baud Rates: 9600 9600 9600
Modem Control: on off
Flow Control: None RTS/CTS
IP Destination:
Netmask:
IPX Network: 00000000
Routing: Broadcast Listen
Compression: Enabled Disabled
PPP Async Map: 00000000
Input Filter:
Output Filter:
Apply Save Remote Reset Default Clone Done

Figure 3-8. Edit Port Window - Hardwired Dialnet

The following parameters are only available for ports which are configured for Hardwired Dialnet connections.

Protocol

This indicates which protocol to use for encapsulating packets. The options are:

PPP - Use PPP with IP packet routing.

PPP/IPX - Use PPP with IPX packet routing.

PPP/IP/IPX - Use PPP with both IP and IPX packet routing.

SLIP - Use the Serial Line Internet Protocol.

MTU

This is the Maximum Transmission Unit to be used for the interface. PPP connections can be set from 100-1500 octets and the remote computer can negotiate a smaller value than the setting entered. SLIP connections can be set from 100-1006. Maximum Transmission Unit defines the largest "frame" or "packet" which can be sent through this connection. If a packet is too large, it will be automatically fragmented. Setting this to smaller values can be useful for the TCP/IP protocol when using multi-line load balancing or for enhanced interactive performance while running large file transfers.

IP Destination

The Internet Protocol Address or a host name of the system at the remote end of the point to point connection should be entered.

Netmask

The netmask of the system at the remote end of the point to point connection should be entered.

IPX Network

The IPX Network Address for the point to point connection should be entered. This value must be in HEX format.

Routing

This indicates whether the PortMaster should use the RIP protocol

through the Interface. Any combination of "Broadcast" and "Listen" can be used. If "Broadcast" is selected, the PortMaster will send RIP information to the remote computer. If "Listen" is selected, the PortMaster will accept RIP information from the remote computer.

Compression

This indicates whether the PortMaster should use Van Jacobson TCP/IP header compression. This option can increase the performance of interactive TCP sessions if both sides of the link support this option. When configuring SLIP connections, both sides must be configured identically. When configuring PPP connections, if compression is enabled and the remote site doesn't support compression, the PortMaster will dynamically disable this feature. Refer to RFC 1144 for detailed information on header compression.

PPP Async Map

The PPP protocol supports the escaping of non-printing ASCII in the data stream. Escaping means that specified characters will not be sent through the line, but instead will be replaced by a special set of characters which the remote site will interpret as the original character. The PPP Async Map is a bit-map of characters which should be escaped. The first (or zero) bit corresponds to the first ASCII character "NULL" and so on. Most environments should be set to zero to achieve maximum throughput.

Input Filter

When the port is specified as a **Hardwired Dialnet** port, this menu item allows you to select from a list of all available input filters on the PortMaster. If specified, all packets received by the specified interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Packet Filters" later in this chapter.

Output Filter

When the port is specified as a **Hardwired Dialnet** port, this menu item allows you to select from a list of all available output filters on the

PortMaster. If specified, all packets being sent to the specified interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Packet Filters" later in this chapter.

Enabling Serial Port Parameters

If you would like to try a new port configuration without saving to the PortMaster permanent configuration:

1. Select **APPLY**
2. Select **REMOTE RESET**

The new port configuration will now be in effect until power is removed from the PortMaster or changed again.

If you want to save the new configuration in the permanent PortMaster configuration, select **SAVE**.

Setting the Parallel Port Configuration

This device type is always **Host Device**. For the parallel port to become active, assign a Host Device name (*/dev/<device>*) as described above under the heading "**Host Device**". In "**Extended Mode**" a specific host (other than the default) may be entered for the port. In addition, if a Device Service other than "**PortMaster**" is selected, the port will be accessible as a network attached device in the same way as the serial ports described above.

Managing the IP Hosts Table

Each device attached to the network is assigned a unique internet address. Internet addresses are four byte numerical values. To make it easier to remember these values, most systems on the network support a way of aliasing the internet address to some unique and easy to remember name. This is done on UNIX systems in the /etc/hosts file. The PortMaster also supports the same capability by maintaining a local hosts table.

If the host name specified by the user is not found in the hosts table the PortMaster will attempt to match the host name using either the Network Information Service (NIS), also known as "YP"; or DNS, the Domain Name Service. See the section "Global Configuration" for more information on setting the NIS or DNS server and domain.

To view or edit the PortMaster hosts table, log in to the PortMaster and select the "**Hosts**" button from the main console.

The following window will be displayed:

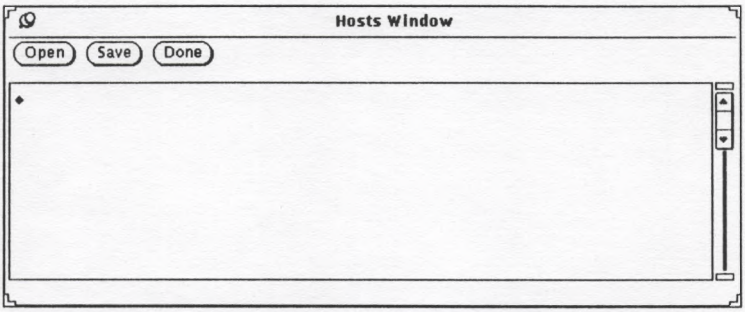


Figure 3-9. Hosts Window

The buttons across the top of the Hosts window are used to access the available functions. The buttons are:

- **Open** - Retrieves the current hosts table from the PortMaster and displays it in the scrollable text window.

- **Save** - Saves the hosts entries shown in the text window as the new hosts table for the PortMaster.
- **Done** - removes the Hosts Window from view.

To edit the PortMaster hosts table use the following general procedure:

1. Select **Open** with the left mouse button. The Hosts table will be retrieved from the PortMaster, sorted in IP address order and will be displayed in the scrollable text window.

2. Make additions, deletions, and changes. All entries should have the Internet address (in the conventional '.' notation) followed by the official host name. A '#' indicates the beginning of a comment; characters up to the end of the line are ignored. This convention is identical to the /etc/hosts file on your UNIX Workstation. Therefore, the /etc/hosts file can be pasted directly into the text window.

3. After making all modifications, select "**Save**". This will store the entries in the text window into the Flash RAM of the PortMaster.

Managing the Users Table

The Users Table provides login security for users to establish login sessions or for incoming Dialnet network connections or for terminal login sessions..

Serial ports configured to accept login sessions initially prompt for a login user name. After receiving the login name, the PortMaster checks the name against the list of names in the local Users Table. If found, the PortMaster initiates password authentication of the user. If the password received matches the password stored in the Users Table, or on the RADIUS server the PortMaster begins the session which has been defined for the user.

Four types of users can be created: **Network User/Normal**, **Network User/Dialback**, **Login User/Normal** and **Login User/Dialback**.

Network User/Normal users are allowed to immediately establish an active PPP or SL/IP connection to the network. **Network User/Dialback** users are disconnected by the PortMaster. The PortMaster then automatically dials to the user's remote modem using a predefined telephone number. **Login User/Normal** users are allowed to immediately begin an active session on a host on the network. **Login User/Dialback** users are disconnected by the PortMaster. The PortMaster then dials to the user's remote modem using a predefined telephone number. This feature allows for enhanced security or for simple telephone charge-back.

If the login name does not match an entry in the Users Table and the port is configured to support **Pass-Thru Login** it automatically forwards the session to the designated host on the local network for password authentication. If your site is using the RADIUS authentication server the validation and login attributes are performed by the server.

To view or edit the PortMaster Users Table, log in to the PortMaster and select the "**Tables**" button from the main console with your right mouse button. A pop-up menu will be displayed. Select "**Users**" from the menu.

The following window will be displayed:

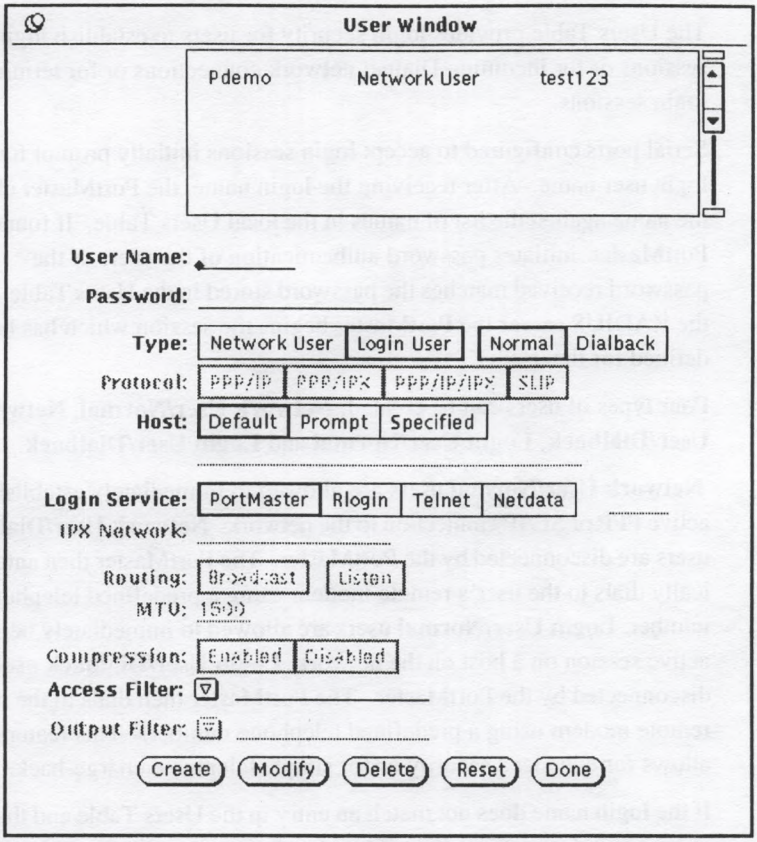


Figure 3-10. Users Window

The mouse buttons across the bottom of the Users window are used to access the available functions. The buttons are:

- **Create** - Add the currently displayed user to the PortMaster Users Table.
- **Modify** - Apply modifications to the user displayed.
- **Delete** - Delete the currently displayed user from the PortMaster Users Table.

- **Reset** - Clear the Users Window to allow the entry of a new user.
- **Done** - Remove the Users Window from the display.

Login User Parameters

The Users Table has 6 fields for each login user and 7 fields for dialback users. These fields are:

User Name

The login name of the user. This name can be up to 8 characters and is the name entered at the "login:" prompt from the PortMaster.

Password

The password for the user. This is a string of up to 16 ASCII characters.

Type

All login users must be set to a type of "**Login User**". Login users can be set to "**Normal**" or "**Dialback**". Normal users will be allowed to immediately begin a login session after properly entering their user name and password. Dialback users will be disconnected by the PortMaster and then re-dialed at their predefined telephone number.

Host

This field defines which network host the user's session will connect to. The three options are:

Default - Connect the user to the defined host for this serial port. Consult the serial port edit window for the defined host.

Prompt - Allow the user to select a host (either by IP address or name) to begin a login session.

Specified - Connect the user to the host specifically entered on the line below the Host selection. A valid host name or IP address should be entered here.

Login Service

The user can be set to use any of the available PortMaster Login

Services. For a complete description of these services, consult the login service descriptions defined in the extended serial port parameters section of this manual.

Telephone No

This field is only displayed for Dialback Login Users. The telephone number which should be dialed to reach the user's modem must be entered in this field. Dialback only supports modems with the Hayes "AT" command set. Only the telephone number is needed, the PortMaster provides the required AT commands.

Access Filter

An optional access control filter can be specified for the user. This filter is taken from the standard packet filter table described later in this chapter. After the user specifies a host, its address is compared against the designated filter. If the address is "permitted" by the filter, the user's connection will be allowed. If not, access will be denied.

Network User Parameters

The User Table is also used to maintain inbound network connections. The fields are similar to those used for Login Users, and there are some additional fields used which are not needed for Login Users. Selecting the Network User button produces the following window:

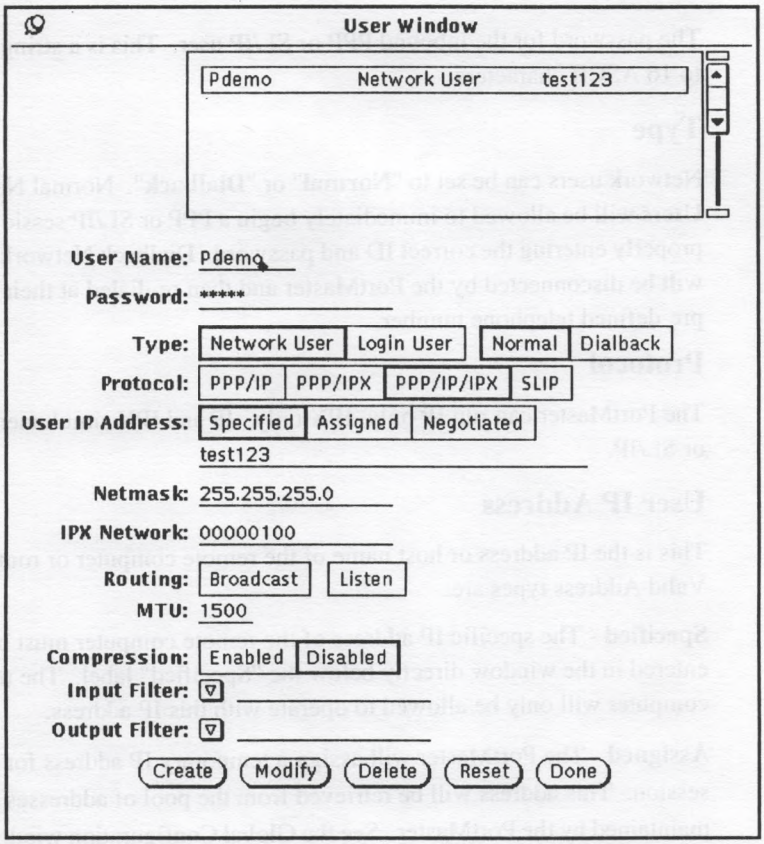


Figure 3-11. User Window - Network Type

User Name

In the case of a Network User, this field is used as the ID of the inbound connection used in a "Chat" style script. For example, the login name used in a Location Table (see "Managing the Location Table" in the next section) script would be the expected ID provided to the PortMaster.

Password

The password for the inbound PPP or SL/IP user. This is a string of up to 16 ASCII characters.

Type

Network users can be set to "**Normal**" or "**Dialback**". Normal Network Users will be allowed to immediately begin a PPP or SL/IP session after properly entering the correct ID and password. Dialback Network Users will be disconnected by the PortMaster and then re-dialed at their pre-defined telephone number.

Protocol

The PortMaster can run IP only, IPX only, IP and IPX simultaneously, or SL/IP.

User IP Address

This is the IP address or host name of the remote computer or router. Valid Address types are:

Specified - The specific IP address of the remote computer must be entered in the window directly below the "Specified" label. The remote computer will only be allowed to operate with this IP address.

Assigned - The PortMaster will assign a temporary IP address for this session. This address will be retrieved from the pool of addresses being maintained by the PortMaster. See the Global Configuration window for more information on Assigned Addresses.

Negotiated - This option is valid only for PPP sessions. The PortMaster will attempt to learn the IP address of the remote computer automatically.

Netmask

The netmask of the system at the remote end of the dial-up connection should be entered.

IPX Network

The IPX network number to be used for the dial-up link should be entered. For remote nodes this will be the unique network for the user. This value must be in HEX format.

Routing

This indicates whether the PortMaster should use the RIP protocol through the interface. Any combination of "Broadcast" and "Listen" can be used. If "Broadcast" is selected the PortMaster will send RIP information to the remote computer. If "Listen" is selected, the PortMaster will accept RIP information from the remote computer.

MTU

This is the desired Maximum Transmission Unit to be used for the Interface. PPP connections can be set to values from 100-1500 bytes and the remote computer can negotiate a smaller value than the setting entered. SLIP connections can be set to values from 100-1006. Maximum Transmission Unit defines the largest "frame" or "packet" which can be sent through this connection. If a packet is too large to fit, it will be automatically fragmented into smaller pieces by the PortMaster. Setting this to smaller (i.e.. less than 300) values can be useful when using multi-line load balancing of IP traffic or for enhanced interactive performance while running concurrent file transfers. For IPX connections this should be left at 1500.

Compression

This indicates whether the PortMaster should use Van Jacobson TCP/IP header compression. This option can increase the performance of interactive TCP sessions if both sides of the link support this option. When configuring SLIP connections, both sides must be configured identically. When configuring PPP connections, if compression is enabled and the remote side doesn't support compression, the PortMaster

will dynamically disable this feature. Refer to RFC 1144 for detailed information on header compression.

Location Name

This is the name of the location stored in the PortMaster Location Table. After authenticating a Dialback Network User, the PortMaster will disconnect the active connection. It will then execute an automatic dial back to the specified location.

Input Filter

When specified as a Network User, this allows you to select from a list of all available input filters on the PortMaster. When specified, all packets received from the serial interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Packet Filters" toward the end of this chapter.

Output Filter

When specified as a Network User, this allows you to select from a list of all available output filters on the PortMaster. When specified, packets being sent to the serial interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Packet Filters" later in this chapter.

PPP Auto-Detect and PAP/CHAP authentication

The PortMaster supports Auto-Detect PPP for use with the PAP and CHAP methods of login authentication. If the device at the remote end of the connection wishes to use PAP or CHAP, when the login or host prompt is provided by the PortMaster the remote device should start sending PPP frames negotiation. This will initiate the requested authentication.

The CHAP challenge process (a practical example)

At the corporate site is a PortMaster with a SNMP sysname of **pm1**. When a remote PortMaster establishes a connection and begins sending PPP frames, **pm1** issues a CHAP challenge. Inside the challenge is an

ID string containing the name **pm1**. An entry for **pm1** is *required* in the PortMaster Users Table on the remote PortMaster.

When the remote PortMaster receives the challenge it does a lookup in its local User Table. Finding the entry, it passes the password through MD5, and forms a response back to **pm1**. Contained within the response is an ID string containing the SNMP sysname of the remote PortMaster. **pm1** then looks in the User Table for the ID of the remote PortMaster, and uses the password for that user to validate the CHAP response received from the remote PortMaster.

If the password comparison is successful, **pm1** will then send a "**CHAP successful**" message back to the remote PortMaster and the connection is complete. If the MD5 comparison fails, a "**CHAP failure**" message is sent to the remote PortMaster and the process repeats.

If the corporate PortMaster wishes to use RADIUS to authenticate the remote PortMaster, the ID string and the password can be stored in the RADIUS users file on the RADIUS server. The password *must* be in clear text in order for the MD5 comparison to succeed, therefore the RADIUS directory (*/etc/raddb* by default) and the files contained in that directory should be set to read-only root.

Each PortMaster involved in this authentication must have an entry in its User Table which contains the SNMP sysname of the other PortMaster. The passwords must be identical.

Note: To clarify, the password for **pm1** is known as a *shared secret*, it is the same password used by the remote PortMaster. The name of the remote PortMaster and an identical password *must* be in the PortMaster User Table on **pm1** or in the RADIUS users table on the RADIUS server for **pm1.**

For more information on the PortMaster authentication decision tree refer to Chapter 6, RADIUS.

Managing the Location Table

The Location Table is used for dial-out network connections to remote sites. Each entry specifies a unique location name, the parameters for the location, and information on how to establish the connection to it.

To view or edit the PortMaster location table, log in to the PortMaster and select the "**Tables**" button from the main console with your right mouse button. A pop-up menu will be displayed. Select "**Locations**", the following window will be displayed:

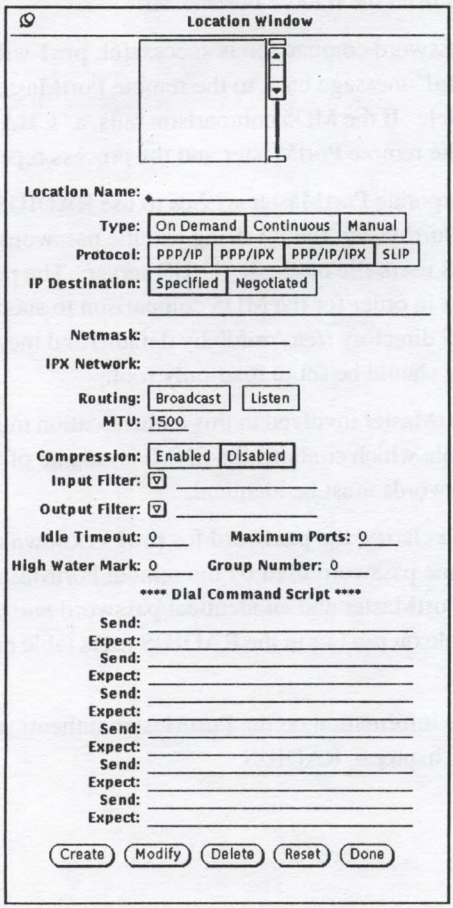


Figure 3-12. Locations Window

The buttons across the bottom of the Locations window access these functions:

- **Create** - Creates a new location table entry based on the fields filled in on the location window.
- **Modify** - Changes the parameters for the location selected in the top location list window to match those filled in on the location window.
- **Delete** - Removes the selected location from the location table.
- **Reset** - Clears the fields on the location table window.
- **Done** - Removes the window.

To create a new location, simply fill in all of the fields in the location window and select the "**Create**" button.

To modify an existing entry, first select that entry with your mouse (by clicking on the entry with the left button) from the selection list. Make the necessary changes. Then select "**Modify**".

To delete an existing entry, select the entry with your mouse (by clicking on the entry with the left button) from the selection list. Select "**Delete**".

Location Table Parameters

These are the parameters which can be edited from this window:

Location Name

The name of the remote location. This can be any 12-character name to identify the remote location. It is generally not the name of a single system, but rather an identifier which represents the entire location (i.e., the city or the company name at that location).

Type

On Demand - This selection notifies the PortMaster to dial and establish a connection to the remote location only when packets are queued for that location. In this mode the PortMaster creates a network interface and the appropriate routing information to notify the attached local area network of the connectivity to the remote site. This is done even though there may not be an actual physical connection to that site at the time.

Continuous - This selection notifies the PortMaster to always keep the dial-up connection to the remote site active. If the telephone line is lost, the PortMaster will automatically initiate a re-dial to that location.

Manual - This selection notifies the PortMaster to only dial to the remote location when an operator requests the connection. This can be done from the **pmconsole** Dialer Window or it can be invoked from the "**pmdial**" program installed on one of the workstations on the network. This also allows connections to be scheduled by using the UNIX cron scheduler to call pmdial.

Note: *When switching a location from Manual to On-Demand make sure the dial-out connection has been closed (reset the serial port) before updating the location table.*

Protocol

This indicates which protocol to use for encapsulating packets. The options are:

PPP/IP - Use the Point to Point Protocol with TCP/IP.

PPP/IPX - Use the Point to Point Protocol with IPX.

PPP/IP/IPX - Use the Point to Point Protocol with TCP/IP and IPX.

SLIP - Use the Serial Line Internet Protocol.

IP Destination

For SLIP connections, enter the IP Address or the host name of the system at the remote end of the dial-up connection.

For PPP connections the Destination can be negotiated. In this mode the PortMaster learns the IP address of the remote system. This feature should only be used for manual or continuous connections. On-Demand locations must use a specified address.

Netmask

The netmask of the system at the remote end of the dial-up connection should be entered.

IPX Network

This is the IPX network number assigned to point to point connection. This value must be in HEX format.

Routing

This indicates whether the PortMaster should use the RIP protocol through the Interface. Any combination of "Broadcast" and "Listen" can be used. If "Broadcast" is selected, the PortMaster sends RIP information to the remote computer. If "Listen" is selected, the PortMaster will accept RIP information from the remote computer.

MTU

This is the desired Maximum Transmission Unit to be used for the Interface. PPP connections can be set from 100-1500 bytes and the remote computer can negotiate a smaller value than the setting entered. SLIP connections can be set from 100-1006. Maximum Transmission Unit defines the largest "frame" or "packet" which can be sent through this connection. If a packet is too large to fit it will be fragmented into smaller pieces. Setting this to a value less than 300 can be useful when using multi-line load balancing or for enhanced interactive performance while running concurrent file transfers.

Compression

This indicates whether the PortMaster should use Van Jacobson TCP/IP header compression. This option can increase the performance of interactive TCP sessions if both sides of the link support this option. When configuring SLIP connections, both sides must be configured identically. When configuring PPP connections, if compression is enabled and the remote side does not support compression the PortMaster will dynamically disable this feature. Refer to RFC 1144 for detailed information on header compression.

Input Filter

When specified as a Network User, this allows you to select from a list of all available input filters on the PortMaster. When specified, all packets received by the specified interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Packet Filters" later in this chapter.

Output Filter

When specified as a Network User, this allows you to select from a list of all available output filters on the PortMaster. When specified, all packets being sent to the specified interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Packet Filters" later in this chapter.

Idle Timeout

For Manual and On-Demand type locations this specifies the number of minutes the line should be idle (no network traffic to the remote site) before disconnecting the telephone connection.

Maximum Ports

The number of dial-out ports the PortMaster can use for this network connection. If 0 is selected dialing to this location will be disabled. If more than 1 is selected the PortMaster will use the "High Water Mark" to decide when to open and dial additional lines. If more than one line is open to the remote location the PortMaster will use load balancing to achieve the maximum throughput of all lines combined. If multiple lines are open the "Idle Timeout" value will be used to decide when to disconnect unneeded lines.

High Water Mark

The number of bytes of queued network traffic required to open an additional dial-out line to the remote site. This value is only used when the "Maximum Ports" is greater than 1 and there are available modems

on the PortMaster. Setting a very small number will cause the PortMaster to quickly use all of the ports specified in "Maximum Ports". Generally, interactive terminal traffic has no more than a few hundred bytes queued at any one time. However, file transfers (i.e., ftp) will queue several thousand bytes. These size differences should be used when deciding what number to use for the High Water Mark.

Group Number

The modem pool group to which this location is assigned. Only modem ports which are configured with this Group Number will be available for dial-out to this location. This is used to reserve modems for dial-up to specific locations or to separate different types of modems requiring compatibility with the remote location.

Dial Command Script

This script is used to issue commands to the modem (or other similar equipment) to dial a number and establish a link. In addition, this script is used for authentication (password security) at the remote site. Each "Send" string is issued out of the PortMaster to the modem or remote computer. Each "Expect" string is used by the PortMaster to verify that the previous "Send" string was properly received by the modem or remote computer and the PortMaster should transmit the next "Send" string.

Send - This string can be up 30 characters in length. Any printing ASCII character can be placed in this string. In addition, the following special characters are available:

\r - This is replaced by the ASCII carriage return character.

\n - This is replaced by the ASCII line feed character.

\0XX - This is replaced by the octal digit specified in the XX.

\\ - This is replaced by the single backslash (\) character.

Send strings must end with the "\r" character.

Expect - This string can be up to 30 characters in length. Any printing

ASCII character can be placed in this string. In addition, any of the special characters from above can be used. Generally, a valid reply can be determined by checking for the last word received from the remote system. For example if the remote system is prompting for a login id, it may issue the string:

```
Please enter your login:
```

The Expect string in the Dial Command Script could simply look for "login:".

It is recommended that the last entry in the Dial Command Script be an Expect string which indicates that the remote location is ready to begin receiving network packets. This is used to activate the data link protocol coming from the PortMaster. When connecting to a remote PortMaster the final reply string to look for should be "SL/IP" for SLIP connections and "PPP" for PPP connections. For other products, consult that vendor's user's manual.

The following Dial Command Script is an example of how to establish a connection between two PortMasters which have modems supporting the "AT" dial command syntax:

```
  Send: ATDT18005551212\r
Expect: CONNECT
  Send: \r
Expect: login:
  Send: my_location_name\r
Expect: ssword:
  Send: my_password\r
Expect: PPP
  Send:
Expect:
  Send:
Expect:
```

The "18005551212" would be replaced by the actual telephone number of the remote modem. "my_location_name" would be replaced by the actual user name for your location. "my_password" would be replaced by the actual password set up at the remote site which corresponds to the user name.

PPP CHAP authentication

The PortMaster supports CHAP method of login authentication. If there is a PortMaster at the remote end of the connection, it will immediately begin the PPP negotiation once the connections is established. The PortMaster supports login authentication through CHAP protocol from the remote device; when it receives the challenge, it uses the id string (the remote system name) contained in that challenge to locate an entry in the local User Table. It will then use the user it finds to construct the correct authentication response to the challenge. Refer to the detailed discussion on PAP and CHAP authentication earlier in this chapter.

Dialing Out to Remote Locations

On-demand or **Continuous** dial-out locations automatically initiate dialing to a remote location. **Manual** connections require a system administrator or a scheduler to initiate dial-out connections. **pmconsole** provides a facility for the system administrator to initiate the dial-out operation and if necessary to monitor the progress of the dial-out operation.

When setting up a new **On-demand** location it is recommended to first set up the location as a **Manual** dial-out site for testing purposes and then later switch the location type to **On-demand**.

*Note: When switching a location from **Manual** to **On-demand**, make sure the dial-out connection has been closed (reset the serial port) before updating the location table.*

To initiate dial-out connections via a scheduler (i.e., cron in UNIX systems) or from a UNIX command line prompt see the "**pmdial**" command in the Utilities section of this manual.

To dial to a remote location from **pmconsole**, select the "**View**" button from the main console with your right mouse button. A pop-up menu will be displayed. Select "**Dialer**" from the menu. The window in Figure 3-13 will be displayed.

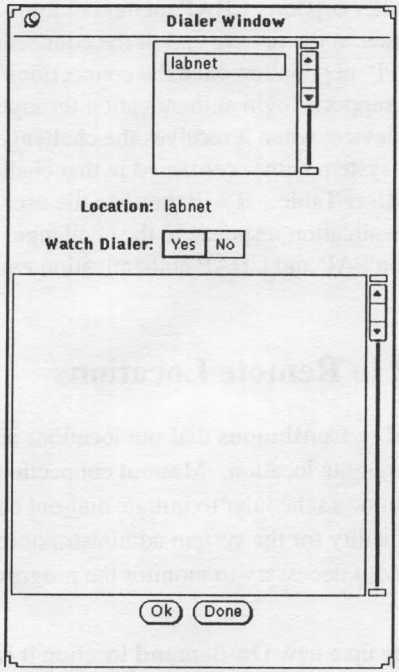


Figure 3-13. Dialer Window

The scrollable list at the top of the window shows all location names which have been set up as "**Manual**" dial-out sites.

Below the list of locations are two fields:

Location

This is the location to dial. This field is filled in by selecting one of the locations from the scrollable list with the left mouse button.

Watch Dialer

Yes - Causes the PortMaster to start dialing and display the progress of the Dial Command Script in the window below.

No - Causes the PortMaster to start dialing the location and immediately returns control to **pmconsole** for another operation.

The mouse buttons across the bottom of the Dialer window are used to access the available functions. The buttons are:

Ok - Begin dialing the specified location.

Done - Dismiss this window.

To begin dialing to a remote location select that entry with your mouse (by clicking on the entry with the left mouse button) from the selection list. The location name will be filled in. Then select "**Yes**" or "**No**" as the monitoring option. Finally, select "**Ok**" from the buttons at the bottom of the window.

If "**Yes**" was selected in the Watch Dialer field the message window will show the location being dialed and the modem port being used. It will then show the execution of the Dial Command Script. The "Send" message shows the exact string of characters being sent out the serial port to the modem or remote system enclosed in parentheses. The "Expect" message shows the response string the PortMaster is expecting as a reply enclosed in parentheses. Immediately following the "expect" string are the characters actually being received by the PortMaster from the modem or remote system. When the PortMaster successfully receives the string is is searching for, it will display ":got it" followed by the next send message.

If the dial script completes successfully the message "Connection Succeeded" will be displayed. Otherwise after timing out the message "Connection Failed" will be displayed

Managing the Routes Table

The PortMaster Routes table is used when static network routes are required. Static routes are required when the user chooses not to run the Routing Information Protocol (RIP) on the PortMaster, or when hosts or networks attached to the PortMaster cannot run the RIP protocol. There are two static routing tables maintained by the PortMaster. One is for IP and the other is for IPX. IP routes contain three entries:

Destination - This is the host or network to which the PortMaster will be required to send packets.

Gateway - This is the directly connected host through which packets should be forwarded to reach the above destination.

Metric - This is a metric representing the cost of sending the packet through the above gateway. Generally metric is the HOP count to the remote network. The number of gateways the packet must cross to reach its destination.

IPX routes contain four entries:

Destination - This is the IPX network to which the PortMaster will be required to send packets.

Gateway - This is the directly connected host through which packets should be forwarded to reach the above destination. It is represented by the combination of network number and node address separated by a colon (i.e., 00001234:00AABBCCDDEE).

Metric - This is a metric representing the cost of sending the packet through the above gateway. Generally metric is the HOP count to the remote network. The number of gateways the packet must cross to reach its destination.

Ticks - This is a number representing the time it takes to send the packet to its destination network in 50ms increments.

To view or edit the PortMaster routes table, log in to the PortMaster and select the "**Tables**" button from the main console with your right mouse button. A pop-up menu will be displayed. Select "**Routes**" from the menu.

The following window will be displayed:

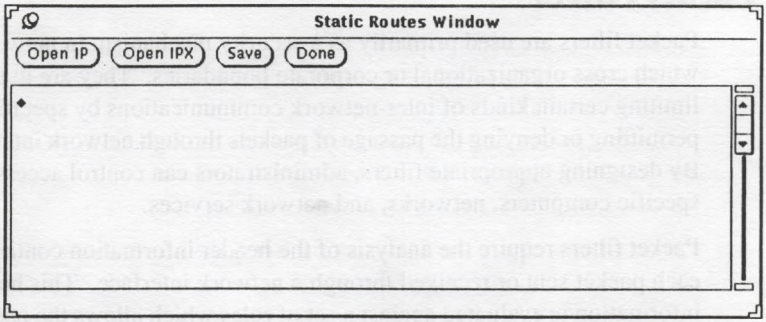


Figure 3-14. Routes Window

The mouse buttons across the top of the Routes Window are used to access the available functions. The buttons are:

- **Open** - Retrieves the current routes table from the PortMaster and displays it in the scrollable text window.
- **Save** - Saves the routes entries shown in the text window as the new routes table for the PortMaster. New routes are entered into the internal routing table on the next update.
- **Done** - Remove the Routes Window from the display.

To edit the PortMaster routes table use the following procedure:

1. Select **Open** with the left mouse button. The Routes table will be retrieved from the PortMaster, sorted in destination name order and will be displayed in the scrollable text window.

2. Make additions, deletions, or changes. Entries must have destination host name, network name, or Internet address (in the conventional '.' notation or the name from the /etc/hosts file or the /etc/networks file) followed by the gateway name (in the same format). A '#' indicates the beginning of a comment; characters to the end of the line are ignored.

3. After making all modifications, select "**Save**". This will store the entries in the text window in the non-volatile configuration of the PortMaster.

Packet Filters

Packet filters are used primarily as a security mechanism in networks which cross organizational or corporate boundaries. They are useful in limiting certain kinds of inter-network communications by specifically permitting or denying the passage of packets through network interfaces. By designing appropriate filters, administrators can control access to specific computers, networks, and network services.

Packet filters require the analysis of the header information contained in each packet sent or received through a network interface. This header information is evaluated against a set of rules which allows the packet to pass freely through the interface (and on to its destination in the network) or causes the packet to be discarded without forwarding.

The Livingston packet filtering mechanism is designed around two primary objectives. First, maximum flexibility is required to allow the administrator to achieve the desired results without compromising security. Second, efficiency is desirable to maximize network performance. Specific features which support these objectives are:

- **Input** and **Output** Filters - Each interface can be assigned both an input-packet filter and an output-packet filter. This is especially useful in routers with more than two network interfaces and it simplifies the design task. The administrator can evaluate each interface for its destination and the mix of inbound and outbound traffic desired for the interface. This capability also has the potential to decrease the number of rules in the filter because fewer network numbers are needed.

- **Source and Destination Address Filtering** - Both source and destination addresses are evaluated in the rule list. Also, the number of significant bits to use in IP address comparisons can be set. This allows filtering based on specific hosts, subnets, or network numbers.

- **Protocol Filtering** - Specific protocols can be handled separately in the packet filters. These include IPX and TCP, UDP, and ICMP for IP.

- **Source and Destination Port Filtering** - The source and destination port numbers can be used in the rule set to control availability of specific network services. This includes evaluation based upon whether the port number is less than, equal to, or greater than a specific value.

- **Established Session Filtering** - The status of TCP connections can

be used as part of the rule set. This allows users in a network to open connections to external networks without allowing external users access to the local network.

- **Unlimited Number of Rules** - Each filter can have a large number of rules specified. This is only limited by available memory within the PortMaster.

- **Simple Rule Creation** - The command syntax for creating specific rules allows the administrator to specify only as much information as is necessary to specify the rule. For example, if the rule is not based upon specific source and destination address, these addresses can be omitted from the specification of the rule.

- **In-line Rule Processing** - Rules are processed in the order they are specified in the rule set. This eliminates ambiguity about how a packet is handled, and allows more flexibility in the creation of a packet filter.

Filter Organization

The PortMaster maintains a table of packet filters in its permanent configuration memory. These filters can be created or modified at any time and are independent of any active packet filters. Each filter is assigned a name of up to 15 characters in length. Each packet filter has three sets of rules. These are IP rules, IPX rules and SAP rules. Each rule set is made up of a list of rules which are numbered starting at 1. A packet filter when initially created contains no rules.

IP and IPX packet filters are "attached" to interfaces as either input or output filters. SAP filters are attached only as output filters. For serial interfaces, the packet filter is enabled when it transitions to the UP state (i.e., after a reset on the port). The Ethernet interface filter is enabled as soon as the name of the input or output filter is specified.

Managing the Filter Table

From the "**Tables**" pop-up menu, select "**Filters**". The screen below

will be shown:

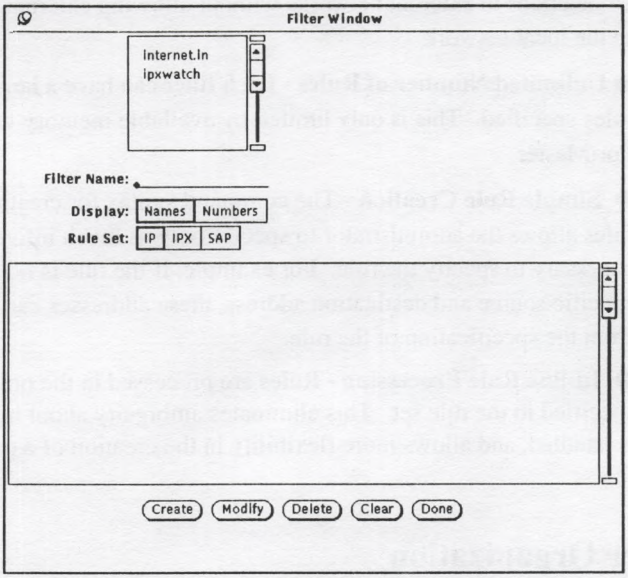


Figure 3-15 Filter Window

The buttons across the bottom of the Filter window are used to access the available functions. The buttons are:

- **Create** - Adds the displayed filter to the PortMaster Filter Table.
- **Modify** - Applies modifications to the filter displayed on the Filter Window.
- **Delete** - Deletes the currently displayed filter from the PortMaster Filter Table.
- **Clear** - Clears the Filter Window to allow the entry of a new filter.
- **Done** - Removes the Filter Window from the display.

Filter Name

This field displays the name of the current packet filter being edited or the name of the new filter being created. Selecting a name from the scrolling list above will fill in the Filter Name.

Display

The display field can be changed at any time and is only used for IP filters. When set to "Names", the rules will convert IP address to host names and port numbers to service names. When set to "Numbers", IP addresses will be displayed in standard dot notation and services will be displayed numerically.

Rule Set

The Rule Set should be set to the type of filter which requires editing. After completing an edit, the rule set should be saved before beginning the edit of a new filter or a different rule set in the same filter.

Filter Rule Syntax

The rule set for the filter is entered on a scrollable text window. Entries can be inserted, deleted, and moved around within this window. Because packets are evaluated in the same order as the rules are listed, the most common packets which will be handled by the PortMaster should be specified first. As soon as a packet matches a rule the action specified by the rule will be taken. If the packet does not match any rule, the action will be to deny the packet from traveling through the interface.

IP Rules

The syntax for specifying an IP rule is:

action [source_address/bits destination_address/bits] protocol options

Actions are specified as the first entry in a rule. Valid actions are:

permit - Permit the packet to pass freely through the interface.

deny - Stop the packet from traveling through the interface.

Source_address/bits - Specifies the comparison with the source IP Address contained in the packet. The number of bits (0-32) are first extracted from the IP Address in the packet (i.e., if 24 bits is specified, a packet with the source address of 192.9.200.1 would become 192.9.200.0 since 24 bits are used to represent the first 3 bytes of the address). The most common bit counts would be:

0 - To match packets with any source IP Address.

16 - To look at only the network number of a class B IP Address.

24 - To look at only the network number of a class C IP Address.

32 - To look at the entire IP Address.

The resulting value is then compared with the source address in the rule.

Destination_address/bit - Specifies the comparison with the destination IP Address contained in the packet. The number of bits (0-32) are first extracted from the IP Address in the packet. The resulting value is then compared with the destination address in the rule.

Protocol - The protocol of the packet may be specified. Valid values are TCP, UDP or ICMP.

Options - Each protocol supports a specific list of options:

TCP - This type of rule supports filtering on source and destination port numbers as well as the established state of the connection. The syntax for TCP options is:

[src eq|gt|lt port_number] [dst eq|gt|lt port_number] [estab]

Where:

src - indicates a comparison should be made with the source TCP port number.

dst - indicates a comparison should be made with the destination TCP port number.

eq - indicates that the port number in the packet should be tested to see if it is equal to the port number specified in the rule.

gt - indicates the the port number in the packet should be tested to see if it is greater than the port number specified in the rule.

lt - indicates that the port number in the packet should be tested to see if it is less than the port number specified in the rule.

estab - indicates that the packet should be tested to see if it is for an established TCP network connection. If this key word is specified, packets being sent to start new TCP connections would not match this rule.

UDP - This type of rule supports filtering on source and destination port numbers. The syntax for UDP options is:

[src eq|gt|lt port_number] [dst eq|gt|lt port_number]

Where:

src - indicates a comparison be made with the source UDP port number.

dst - indicates a comparison should be made with the destination UDP port number.

- eq - indicates that the port number in the packet should be tested to see if it is equal to the port number specified in the rule.

gt - indicates the the port number in the packet should be tested to see if it is greater than the port number specified in the rule.

lt - indicates that the port number in the packet should be tested to see if it is less than the port number specified in the rule.

ICMP - This type of rule supports filtering on type of ICMP message. The syntax for ICMP options is:

[type icmp_message_type]

Where a comparison is made with the ICMP message type contained in the packet.

IPX Rules

The syntax for specifying an IPX rule is:

action [keyword value] [keyword value] ....

Actions are specified as the first entry in a rule. Valid actions are:

permit - Permit the packet to pass freely through the interface.

deny - Stop the packet from traveling through the interface.

Valid keywords are:

srcnet - Specifies the comparison with the source IPX Network Address contained in the packet. This value should be specified in HEX format.

dstnet - Specifies the comparison with the destination IPX Network

Address contained in the packet. This value should be specified in HEX format.

srchost - Specifies the comparison with the source IPX Node Address contained in the packet. This value should be specified in HEX format.

dsthost - Specifies the comparison with the destination IPX Node Address contained in the packet. This value should be specified in HEX format.

srcsocket - Specifies the comparison with the source IPX socket number contained in the packet. A second keyword indicating the type of comparison must be specified. Valid comparison types are "equal", "lessthan" or "greaterthan". Following the comparison keyword, a numeric value should be specified in HEX format.

dstsocket - Specifies the comparison with the destination IPX socket number contained in the packet. A second keyword indicating the type of comparison must be specified. Valid comparison types are "equal", "lessthan" or "greaterthan". Following the comparison keyword, a numeric value should be specified in HEX format

SAP Rules

The syntax for specifying a SAP rule is:

action [keyword value] [keyword value] ....

Actions are specified as the first entry in a rule. Valid actions are:

permit - Permit the service to be advertised on this interface.

deny - Stop the service from being advertised on the interface.

Valid keywords are:

server - Specifies the comparison with the name of the server which is advertising its service.

network - Specifies the comparison with the server's IPX Network Address. This value should be specified in HEX format.

host - Specifies the comparison with the server's IPX Node Address. This value should be specified in HEX format.

socket - Specifies the comparison with the server's IPX socket number .

A second keyword indicating the type of comparison must be specified. Valid comparison types are "equal", "lessthan" or "greaterthan". Following the comparison keyword, a numeric value should be specified in HEX format.

Filter Table Example

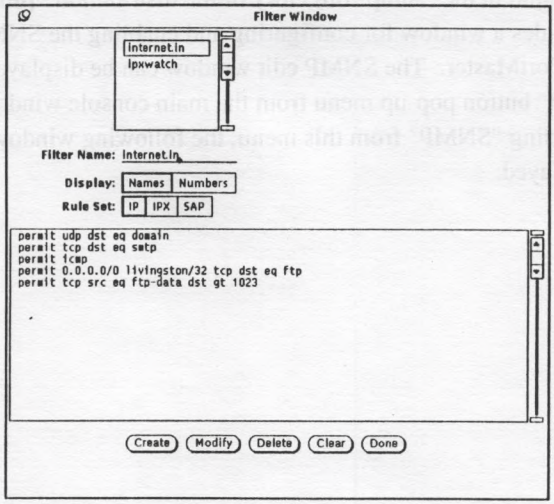


Figure 3-16. Filter Table Example

In figure 3-16, Rule 1 says we permit udp Domain Name Service packets from any foreign host.

Rule 2 says we permit smtp (sendmail) packets.

Rule 3 says we allow icmp (ping) packets.

Rule 4 says we permit ftp from any foreign host but only to "livingston".

Rule 5 works with rule 4 to allow the reverse channel required for the data portion of ftp..

For examples of other filter rules, refer to the "Command Prompt Interface" section of this manual.

Configuring SNMP

The PortMaster provides support for using SNMP for getting and setting network management data. Specifically it provides the industry standard MIB-2 variables. These variables are fully described in the Livingston MIB distributed with the standard Livingston software. This MIB along with configuration files for various network management packages can be found in the "snmp" directory of the distribution. **pmconsole** provides a window for configuring and enabling the SNMP facilities of the PortMaster. The SNMP edit window can be displayed by using the "Edit" button pop-up menu from the main console window. After selecting "SNMP" from this menu, the following window will be displayed:

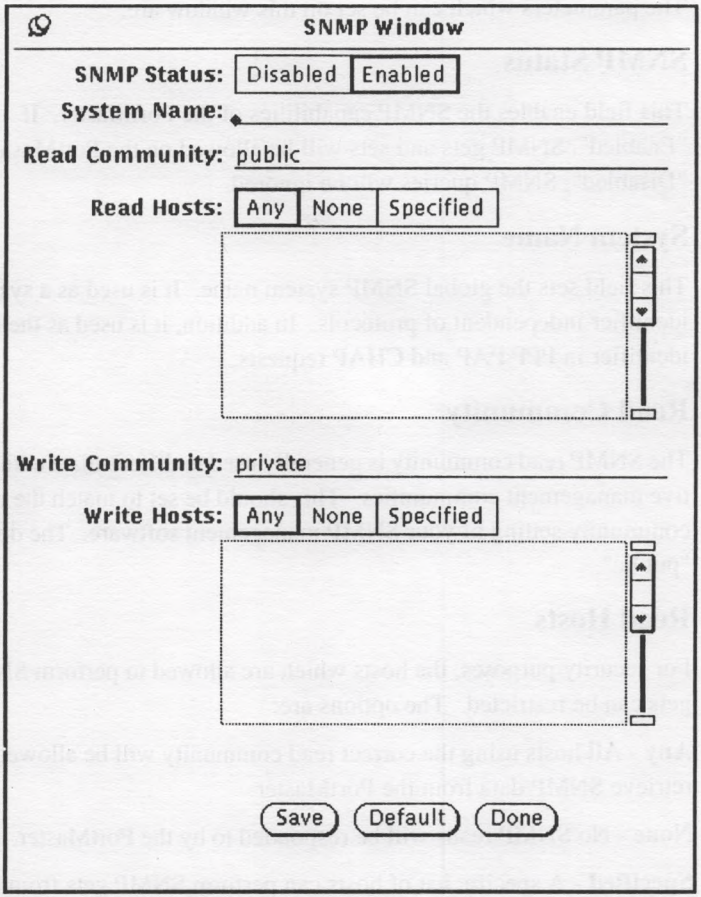


Figure 3-17. SNMP Window

This window has the following buttons:

- **Save** - The currently displayed configuration values will be saved in the non-volatile storage of the PortMaster.
- **Default** - The configuration values will be set to the factory default.
- **Done** - The SNMP window will be removed from the display.

The parameters which can be set on this window are:

SNMP Status

This field enables the SNMP capabilities of the PortMaster. If "Enabled", SNMP gets and sets will be allowed on the PortMaster. If "Disabled", SNMP queries will be ignored.

System Name

This field sets the global SNMP system name. It is used as a system identifier independent of protocols. In addition, it is used as the system identifier in PPP PAP and CHAP requests.

Read Community

The SNMP read community is generally used to differentiate administrative management communities. This should be set to match the read community setting of your SNMP management software. The default is "public".

Read Hosts

For security purposes, the hosts which are allowed to perform SNMP gets can be restricted. The options are:

Any - All hosts using the correct read community will be allowed to retrieve SNMP data from the PortMaster.

None - No SNMP reads will be responded to by the PortMaster.

Specified - A specific list of hosts can perform SNMP gets from the PortMaster. The specific list must be entered in the read hosts window. To edit the list of hosts place your mouse pointer anywhere in the scrolling window. Press and hold the right mouse button to bring up the scrolling list pop-up menu. Select "Edit List". When the scrolling list pop-up menu is accessed again, use the selections to insert, change or delete entries.

Write Community

The SNMP write community is generally used to segregate administrative management communities. This should be set to match the write community setting of your SNMP management software. The default is "private".

Write Hosts

For security purposes, the hosts which are allowed to perform SNMP sets can be set on the PortMaster. The options are:

Any - All hosts using the correct write community will be allowed to set SNMP data on the PortMaster.

None - No SNMP writes will be allowed by the PortMaster.

Specified - A specific list of hosts can perform SNMP sets on the PortMaster. The specific list must be entered in the write hosts window. To edit the list use the same procedure described for "Read Hosts".

RADIUS

The PortMaster supports RADIUS (Remote Authentication Dial In User Service). RADIUS supports authentication of users and remote routers from a centrally managed database maintained on an authentication server. For information on implementing a RADIUS authentication server, see Chapter 6, "RADIUS". **pmconsole** allows an administrator to configure the PortMaster as a RADIUS client. In this configuration, the PortMaster will first consult its local Users Table (See Users Table Maintenance earlier in this chapter), it will then consult the RADIUS server if the user is not locally defined.

From the PortMaster Console Window, select the Edit pop-up menu and select **RADIUS**. The following window will be displayed:

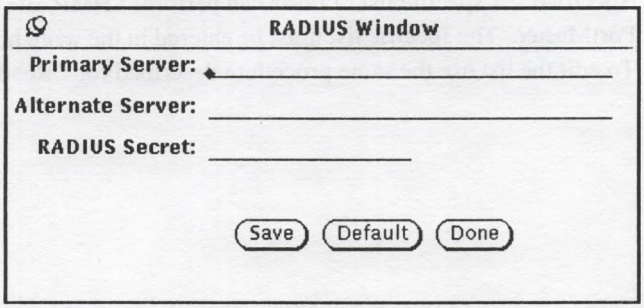


Figure 3-18. RADIUS Window

Primary Server - The host name or the IP address of the Primary Authentication Server.

Alternate Server - The host name or IP address of the Secondary Authentication Server, used when the Primary Server cannot be reached.

RADIUS Secret - Enter the secret used to encrypt users passwords and for verification of the responding RADIUS server. Note that when entering the RADIUS secret from **pmconsole** it is passed over the network in clear text. Alternately this secret may be entered using the command line interface directly through the serial port on the PortMaster.

Monitoring the PortMaster

pmconsole allows the monitoring of traffic, errors, and sessions through the serial ports, as well as monitoring statistics for each of its network interfaces. The View button on the main console window allows selection of either "Ports", "Netstats" or "Sessions".

Port View Window

From the PortMaster Console window, select **View** with your right mouse button. Then select "**Ports**" from the pull-down menu. A window similar to Figure 3-19 will be displayed.

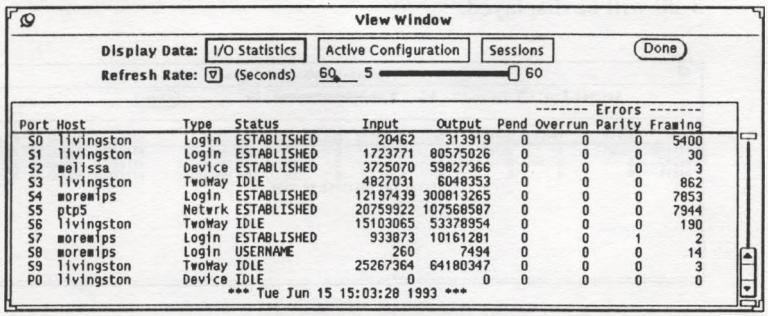

View Window
Display Data: I/O Statistics
Active Configuration
Sessions
Done
Refresh Rate: (Seconds) 60 5 60
Errors
Port Host Type Status Input Output Pend Overrun Parity Framing
S0 livingston Login ESTABLISHED 20462 313919 0 0 0 5400
S1 livingston Login ESTABLISHED 1723771 80575026 0 0 0 30
S2 melissa Device ESTABLISHED 3725070 59827366 0 0 0 3
S3 livingston TwoWay IDLE 4827031 6048353 0 0 0 862
S4 moremips Login ESTABLISHED 12197439 300813265 0 0 0 7853
S5 ptp5 Netwrk ESTABLISHED 20759922 107568587 0 0 0 7944
S6 livingston TwoWay IDLE 15103065 53378954 0 0 0 190
S7 moremips Login ESTABLISHED 933873 10161281 0 0 1 2
S8 moremips Login USERNAME 260 7494 0 0 0 14
S9 livingston TwoWay IDLE 25267364 64180347 0 0 0 3
P0 livingston Device IDLE 0 0 0 0 0 0
*** Tue Jun 15 15:03:28 1993 ***

Figure 3-19. View Window

This window allows you to view the configuration and Status of each port. These values are refreshed at a specific rate as defined by the "**Refresh Rate**" values. Use the slide bar to set the **Refresh Rate**. The **Refresh Rate** slide bar can be set to correspond to either seconds, minutes or hours by choosing an option from the **Refresh Rate** menu.

Three sets of data can be displayed in the view window. These are the "**I/O Statistics**", "**Active Configuration**" and the "**Sessions**". All modes display the port, active host, port type and the status of the port.

When "**Active Configuration**" is selected, the window displays data communications parameters such as baud rate, databits and parity.

When "**I/O Statistics**" is selected the window displays input and output information. There are three columns labeled Input, Output and Pending. These relate to the number of bytes transferred in and out the port and the number of bytes in the PortMaster output buffer which are

pending in the output queue. There are also three error counts displayed: Overrun, Parity and Framing errors.

When "**Sessions**" is selected the window displays active users, the direction in which the connection was initiated, the time since the active session was started, how long the port has been idle, and the idle timeout if one has been set.

Network Statistics

After selecting "**Netstats**" from the pop-up menu, the window in figure 3-20 will be displayed.

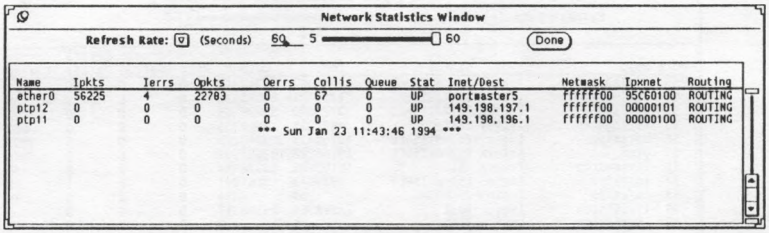

Network Statistics Window
Refresh Rate: (Seconds) 60 5 60
Done
Name Ipkts Ierrs Opkts Oerrs Collis Queue Stat Inet/Dest Netmask Ipxnet Routing
ether0 56225 4 22783 0 67 0 UP portmaster5 FFFFFF00 95C60100 ROUTING
ptp12 0 0 0 0 0 0 UP 149.198.197.1 FFFFFF00 00000101 ROUTING
ptp11 0 0 0 0 0 0 UP 149.198.196.1 FFFFFF00 00000100 ROUTING
*** Sun Jan 23 11:43:46 1994 ***

Figure 3-20. Netstats Window

This window allows you to view the Status of each network interface in the PortMaster. These values are refreshed at a specific rate as defined by the "**Refresh Rate**" values. Use the cycling-arrow icon or the slide bar to set the **Refresh Rate**. The **Refresh Rate** slide bar can be set to correspond to either seconds, minutes or hours by selection with the mouse.

The values which are displayed are:

- **Name** - The name of the network interface. The Ethernet interface is named "ether0" and each interface through the serial ports are named "ptp" or "frm", followed by a uniquely assigned number. "ptp" interfaces are using the PPP or SLIP protocol. "frm" interfaces are using Frame Relay.
- **Ipkts** - The number of input packets received by the interface.

- **Ierrs** - The number of input packets received by the interface which were dropped due to errors.
- **Opkts** - The number of output packets sent by the interface.
- **Oerrs** - The number of output packets which were not sent by the interface due to errors.
- **Collis** - The number of collisions experienced while trying to send packets out the interface.
- **Queue** - The number of packets currently queued for transmission on the interface.
- **Stat** - Either "UP" or "DOWN" indicating whether the interface is active.
- **inet/dest** - For the Ethernet interface, the internet address of the PortMaster. For ptp interfaces, the internet address of the remote system. For frm interfaces, the internet address of the port.
- **netmask** - The netmask of the inet/dest field.
- **Ipxnet** - The IPX network number of the interface.
- **Routing** - "Routing", "Sending", "Listen", or "Quiet" indicating whether RIP protocol packets are being transmitted or received by the interface.

Administration CHAPTER 4

pmconsole with an ASCII Terminal

The ASCII terminal interface provides several screens through which you can configure the PortMaster ports, monitor the performance and install other PortMasters on your network. This can be run from any ASCII terminal logged onto a UNIX workstation which supports full screen addressing and has an entry in the termcap or terminfo database. Before running **pmconsole** verify that your TERM environment variable matches your terminal's entry in the termcap database. If the screen display is unreadable, the wrong terminal type has probably been specified. Press the "Control" key and the letter "C" to exit the program and consult with your system administrator on the proper setting of your terminal type.

When **pmconsole** is started, the screen in Figure 4-1 will be displayed.

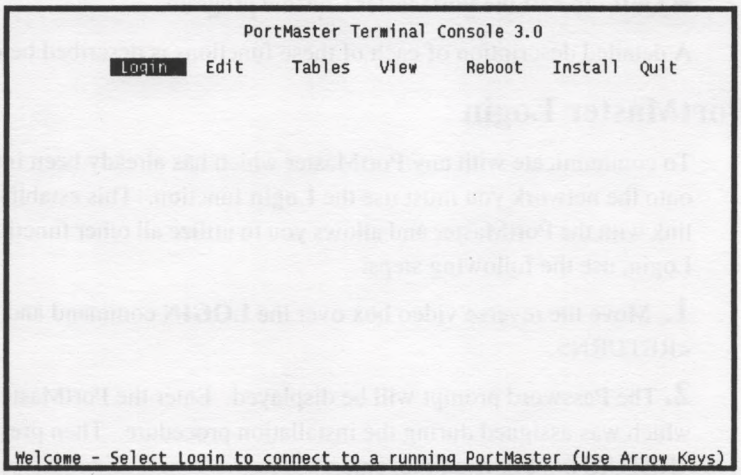

PortMaster Terminal Console 3.0
Login Edit Tables View Reboot Install Quit
Welcome - Select Login to connect to a running PortMaster (Use Arrow Keys)

Figure 4-1. PortMaster Console login display

This is the primary screen in the PortMaster Console program. From this screen all other screens and functions of the software are accessible. The list of commands at the top of the screen are used to access the various functions. A function is selected by using the arrow keys or by typing the first letter of one of the commands. Once the command has been highlighted, pressing the <RETURN> key will cause it to be executed. The PortMaster Console screen has the following commands:

- **Login** - to access any PortMaster.
- **Edit** - to set the port configurations, network configurations, the administration password, SNMP and RADIUS.
- **Tables** - to view and edit Dial-out Locations, User Entries, the Hosts Table, the Static Routing Table or the Filters Table.
- **View** - to view all port configurations, data traffic, active sessions and to establish dial-out connections.
- **Reboot** - to remotely reboot the PortMaster.
- **Install** - to install a PortMaster onto the network or to install new software releases.
- **Quit** - to exit the PortMaster Console program.

A detailed description of each of these functions is described below.

PortMaster Login

To communicate with any PortMaster which has already been installed onto the network you must use the **Login** function. This establishes a link with the PortMaster and allows you to utilize all other functions. To Login, use the following steps:

1. Move the reverse video box over the **LOGIN** command and press <RETURN>.

2. The Password prompt will be displayed. Enter the PortMaster name which was assigned during the installation procedure. Then press <RETURN>. For example, enter:

PortMaster Name: portmaster1

3. Enter the password, if any, and press <RETURN>. When the PortMaster is initially installed there is no password. Then, a message stating that the connection is being attempted will appear. With a successful connection, the main PortMaster screen (Figure 4-2) will be displayed.

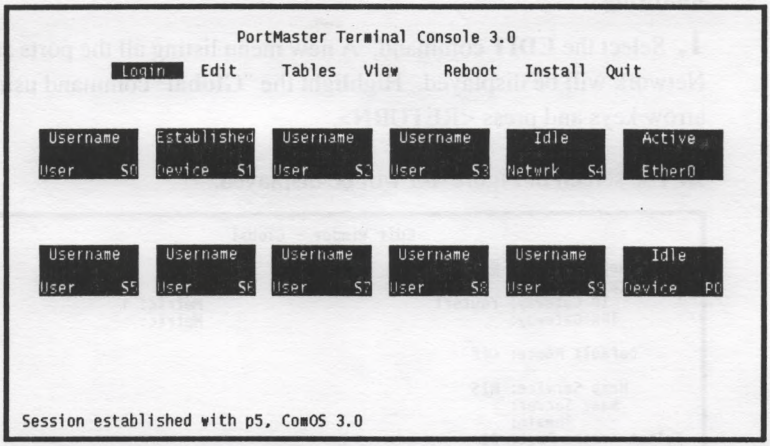

PortMaster Terminal Console 3.0
Login Edit Tables View Reboot Install Quit
Username Established Username Username Idle Active
User S0 Device S1 User S2 User S3 Netwrk S4 Ether0
Username Username Username Username Username Idle
User S5 User S6 User S7 User S8 User S9 Device P0
Session established with p5, ComOS 3.0

Figure 4-2. PortMaster Console screen

The PortMaster Console screen displays the status of the serial ports and the network (Ethernet and Global Configuration).

Global Configuration

This screen is used primarily to set global parameters such as default and alternate hosts, gateways and metrics, and naming service selection. The global configuration window may also be used to change the PortMaster Administration password. From the PortMaster Console, do the following:

1. Select the **EDIT** command. A new menu listing all the ports and the Network will be displayed. Highlight the "**Global**" command using the arrow keys and press <RETURN>.

2. The screen in Figure 4-3 will be displayed.

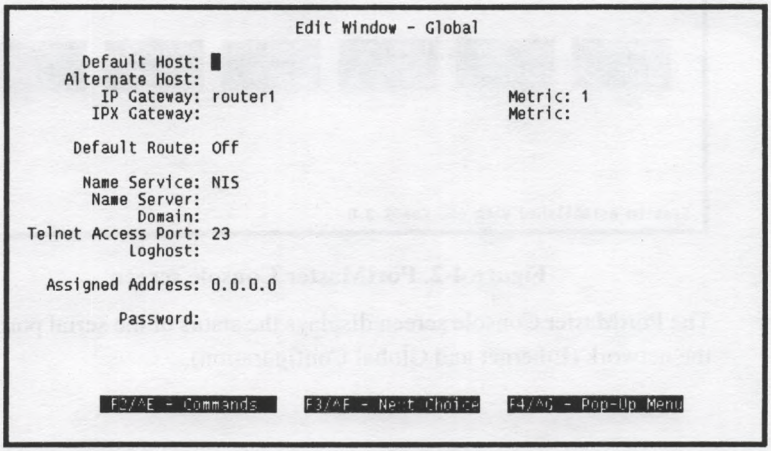


Figure 4-3. Edit screen - Global

3. Enter the following information, terminated by pressing RETURN:

- **Default Host** - Name of the PortMaster host. This is the name of the host the PortMaster uses for login or device services. This is optional and me be left blank.
- **Alternate Host** - Ports configured for User Login will automatically switch to an alternate host if the Default Host is unavailable. This is optional and may be left blank. Up to two additional (for a total of

three) Alternate Hosts may be specified from the Command Prompt Interface (See Chapter 5, "The Command Prompt Interface").

- **IP Gateway** - If the PortMaster is being connected to a network with gateway systems, then the name of the default gateway on the same network should be entered. The PortMaster automatically routes network packets through gateways which are running the Routing Information Protocol (RIP), but will use the default gateway if no RIP gateways are found.
- **IP Gateway Metric** - If the IP Gateway field above is being used, this value (from 1-15) is the hop count associated with using the gateway route. This is useful if the PortMaster is configured to listen for routes coming from other routers. This field can be left blank which assumes a metric of 1.
- **IPX Gateway** - If the PortMaster is being connected to an IPX network with gateways, then the name of the IPX gateway on the same network should be entered. The PortMaster automatically routes network packets through gateways which are running the IPX Routing Information Protocol, but will use the default gateway if no RIP gateways are found.
- **IPX Gateway Metric** - If the IPX Gateway field above is being used, this value is the hop count associated with using the gateway route. This is useful if the PortMaster is configured to listen for routes coming from other routers. This field can be left blank which assumes a metric of 1.
- **Default Route** - This field tells the PortMaster how to manage default routes being sent through the RIP protocol. The following choices are available by using the "Next Choice" or "Pop-Up Menu" function keys:

  On - The PortMaster will send default route information as part of its normal RIP messages and will accept default route information coming from other routers on all configured interfaces.

  Broadcast - The PortMaster will send default route information as part of its normal RIP messages.

  Listen - The PortMaster will accept default route information coming

from other routers on all configured interfaces.

Off - The PortMaster will not send default route information to any configured interfaces and it will ignore all default route messages it receives on any configured interfaces.

- **Name Service** - For networks which use the Network Information Service (NIS), also known as YP, the PortMaster can be configured to use this service for host name matching. Select DNS if your network is configured for Domain Name Service.
- **Name Server** - Enter the name of the server providing the name service selected above.
- **Telnet Admin Port** - The PortMaster allows the system administrator to access all of the PortMaster administration functions through a command line interface. These functions can be reached by logging onto the PortMaster with a telnet session. This field identifies the specific TCP port number for the PortMaster to listen on for incoming telnet administration sessions. The default value is "23". Any number from 0 to 65536 may be used. Ports numbered from 10000 through 10100 are reserved for an internal filter used for outbound security. See Appendix E, "Outbound Security" for more information. If 0 is selected, the PortMaster will disable the telnet administration function.
- **Loghost** - The PortMaster supports the "syslog" network accounting function. If a host is entered in this field, the PortMaster will log authentication information to this host using the system facility "auth" and the priority of "info" (auth.info). Consult your system's syslogd and /etc/syslog.conf manual pages for more information on these services.
- **Assigned Address** - This field is used in conjunction with Dialnet. It is only used for network login users using the PPP protocol who are being assigned a temporary IP address for their active session. If a network user in the passwords table has been set to use an "Assigned Address", the PortMaster must allocate a temporary IP address to be used for their active session. This IP address is retrieved from a pool of addresses maintained by the PortMaster. The IP address entered in

this field will be used as the first free address in the pool of addresses. The PortMaster will allocate as many addresses as there are ports configured for Dialnet access.

- **Password** - PortMaster administration password.

As each of the items is entered, it will be validated against your systems global host table (/etc/hosts, DNS or NIS) of it is an IP host name. These were established by **pminstall** if this is a stand-alone installation, or by your network administrator.

4. You will notice a function key label (F2) at the bottom of the screen. This indicates that by pressing function key F2 or by pressing down the "Control" key and typing the letter "E" the commands menu will be displayed. To save the configuration data in the PortMaster, press F2 and select **SAVE** from the command list. At the bottom of the screen will be a message:

Configuration successfully saved.

5. Select the DONE command. At this point, the PortMaster has all the information necessary to begin normal communications with the network.

Ethernet Port Configuration

To configure the ethernet port use the following procedure:

1. Select the **EDIT** command. A new menu listing all the ports and the Network will be displayed. Highlight the "**Ether0**" command using the arrow keys and press <RETURN>.

2. The screen in Figure 4-4 will be displayed.

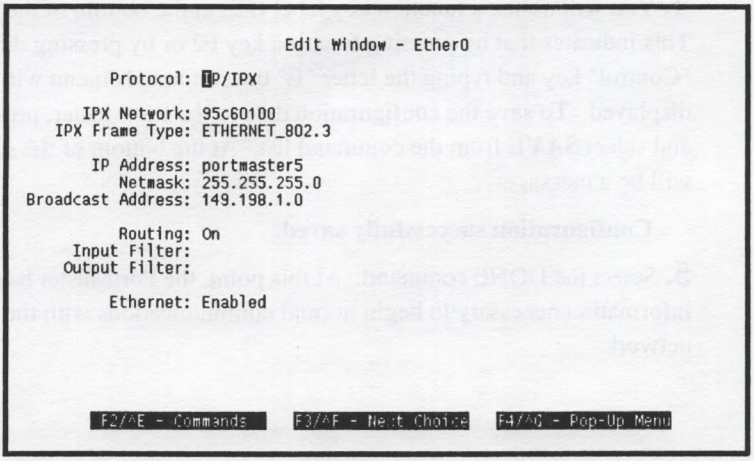


Figure 4-4. Edit Window - Ether0

- **Protocol** - select one of IP, IPX, or IP and IPX. If IPX or IP/IPX is selected, you must fill in the following two entries:

- **IPX Network** - enter the address of your IPX network.

- **IPX Frame Type** - specify the ethernet frame type. This should be set to match the frame type of Novell servers and clients.

- **IP Address** - IP address for the PortMaster entered during installation.

- **Netmask** - defaults to 255.255.255.0. This should only be modified if your site uses sub-netting or Class A or B IP addresses. Consult

you network administrator for this information.

- **Broadcast Address** - This is the IP address which the PortMaster will interpret and use as the local broadcast address. This is used by the RIP protocol and some diagnostic protocols. This value *must* match other computers on the same local Ethernet. This can be selected by using the "Next Choice" function key.

- **Routing** - This indicates whether the PortMaster should use the RIP protocol through the Ethernet Interface. The default is for the PortMaster to both Broadcast and Listen for Routing Information Protocol packets on the local Ethernet. The following choices are available by using the "Next Choice" or "Pop-Up Menu" function keys:

  On - The PortMaster will send RIP information to other computers attached to the local Ethernet and will accept RIP information from other routers on the local Ethernet.

  Broadcast - The PortMaster will broadcast RIP information to other computers attached to the local Ethernet.

  Listen - The PortMaster will listen for RIP information from other routers on the local Ethernet.

  Off - The PortMaster will not send RIP information to the local Ethernet and it will ignore all RIP messages it receives on the local Ethernet.

- **Input Filter** - Allows you to select from a list of all available input filters on the PortMaster. When specified, all packets received from the specified interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Packet Filters" toward the end of this chapter.

- **Output Filter** - Allows you to select from a list of all available output filters on the PortMaster. When specified, all packets being sent to the specified interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Packet Filters" toward the end of this chapter.

- **Ethernet** - This field enables IP traffic on the Ethernet interface of the PortMaster. It should only be disabled when the PortMaster is not being attached directly to the local Ethernet. This can be selected by using the "Next Choice" function key.

Installation from PortMaster Console

To install a PortMaster from the PortMaster Console, instead of using the program **pminstall** as described in Chapter 2, select the **INSTALL** command. The screen in Figure 4-5 will appear. The option commands in this screen are the same options available with **pminstall** (See Chapter 2, Running **pminstall**):

- New PortMaster
- New Host
- Upgrade PortMaster
- Upgrade Host
- Done

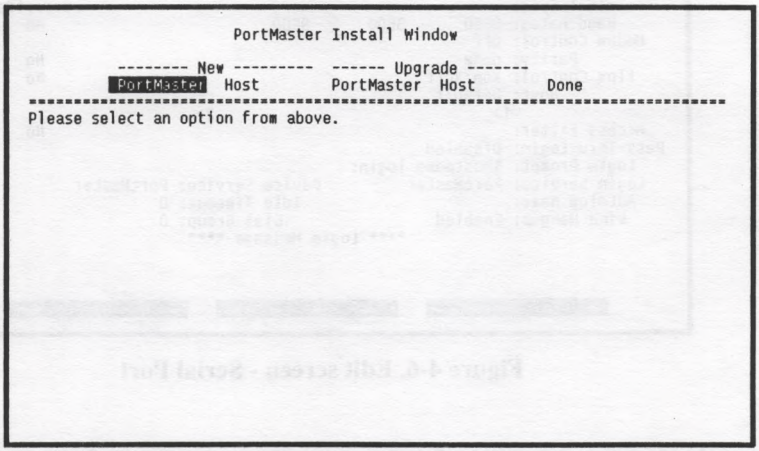


Figure 4-5. PortMaster Install screen

Serial Port Configuration

To set the configuration of ports S0 through S29, use the following procedure:

1. Select the **EDIT** command. A new menu listing all of the ports and the Network will be displayed. Highlight the Serial Port using the arrow keys and press <RETURN>.

2. The Edit screen for all ports (Figure 4-6) will appear. From this screen you can modify the serial port configuration parameters.

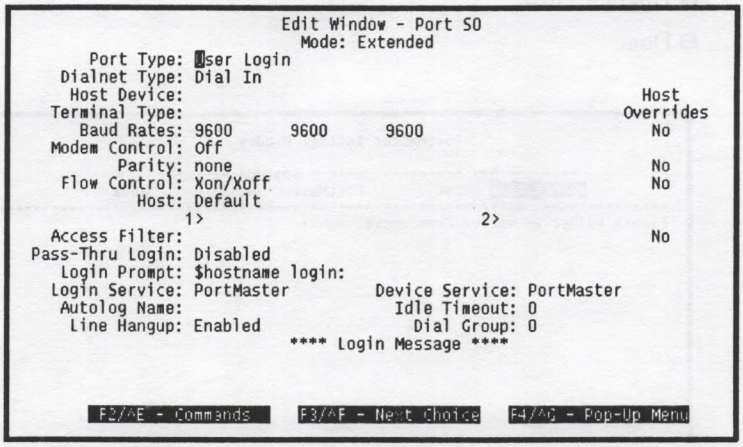


Figure 4-6. Edit screen - Serial Port

Upon entry, you will be in edit mode. This means that you can move around the screen with the arrow keys or by pressing <RETURN>. In addition, there is a set of function key labels across the bottom of the screen. Any of these function keys (or their associated Control characters) can be pressed at any time. When the F2 or "Control-E" key is pressed, the function key is replaced by a menu of commands which can be executed. The available commands are:

- **APPLY** - send the configuration to PortMaster memory. Does not take effect until you select **RESET**. These values are temporary until you select **SAVE**. If power is removed from the PortMaster, or if the PortMaster is rebooted prior to selecting **SAVE**, the new parameter values will no longer be stored in the PortMaster.
- **SAVE** - performs an **APPLY** and stores the port configuration in the PortMaster non-volatile storage.
- **RESET** - reset the serial port using the values stored by the **APPLY** or **SAVE** selection.
- **GENERIC** - set the *on-screen* values to the port default configuration.
- **CLONE** - copy the port configuration from another port.
- **EDIT** - returns you to edit mode. The cursor moves back up onto the screen and the function key labels re-appear.
- **DONE** - return to the PortMaster Console screen.

Serial Port Parameters

This screen displays the serial port parameters and the current values. Some selections have menus. To use the menus, move your cursor to the field to be changed with the <RETURN> or arrow keys. Press the F4 function key (or Control-G) and a menu of choices will be displayed. Alternately the selections can be rotated through with the F3 function key (or Control-F). Other items can be edited directly from your keyboard by typing in new choices.

The serial port edit screen supports two modes of operation; "**Standard**" and "**Extended**". Many users will find that the "**Standard**" mode will meet all of their needs. "**Extended**" mode is for users who wish to customize the operation of the serial port more extensively. The desired mode can be selected by choosing a **Mode** option at the top of the edit screen.

Standard Mode Parameters

These are the parameters that can be selected from this screen:

Port Type *(menu field)*

User Login (default) - The specified port will display a login prompt to the user. After successful baud rate matching and receiving a login name, the user will either be authenticated from the PortMaster passwords table, the RADIUS Authentication Server, or will be transferred directly to a login session on the host workstation.

Host Device - The port will operate as a host controlled device on the host workstation or as a network accessible device using telnet, rlogin, or a binary TCP connection (See "Device Service" in Extended Mode Parameters later in this chapter).. The Host Device field described below must be entered.

Two-Way - The port will operate in User Login mode if carrier is detected on pin 8 of the RS-232 connector. Otherwise it can be accessed as a host device. The Host Device field described below must be entered.

Dialnet - This option can be selected in combination with the other Port Types if the "**Dialnet Type**" field is set to a value other than "**Hardwired**". The port becomes available for running the Serial Line Internet Protocol (SL/IP) or the Point to Point Protocol (PPP) for establishing connections between remote sites over modems. The specific services are defined in the following "Dialnet Type" field.

Dialnet Type

Hardwired - The port is being used for a dedicated network connection between two sites. No modem dialing or authentication is required. The port immediately begins running the specified protocol. In this mode, none of the other port types can be used in combination with Dialnet.

Dial In - In this mode, the port will accept dial-in only network connections. The remote system (or user) will be required to enter a user id and password. Dial In network connections are controlled by the User Table described later in this chapter.

Dial Out - In this mode, the port becomes available for dialing to remote destinations and initiating network connections to those destinations. Dial Out network connections are controlled by the **Location Table** described later in this chapter.

Dial In & Out - In this mode, the port will accept dial-in network connections, as well as being available for dial out to remote destinations. In any of the three Dial modes the port can also be configured to support other port operations concurrently. If one of the other port types is selected, both that port type and **Dialnet** will be highlighted. If one of the other port types is selected, additional configuration parameters become available.

Host Device *(keyboard entry field)*

This is field will be displayed in either the **Host Device** or **Two-Way** modes. The Host Device name is the name of a pseudo tty device in the workstation directory /dev. Standard device entries are:

/dev/ttyp0 - /dev/ttypf
/dev/ttyq0 - /dev/ttyqf
/dev/ttyr0 - /dev/ttyrf

Since other programs on the host computer use these same pseudo tty devices, care should be taken in selecting the devices for the PortMaster. Each PortMaster port that binds to a specific device should be allocated a unique device name. In addition, since most dynamically allocated devices are taken from the beginning of the above list, it is recommended that devices at the end of the list be used for the PortMaster. See Appendix A for discussion of device drivers.

When using the port as a network accessible device using rlogin, telnet, or netdata, this entry should be set to "/dev/network".

Terminal Type *(keyboard entry field)*

This optional field is used in either the **User Login** or **Two-Way** modes.

When a new session is established on the host workstation, this terminal type will be set in the user's environment. A valid entry from the termcap file should be entered. If this field is left blank, the host computer will assume a "dumb" terminal.

Baud Rates *(menu field)*

Three different baud rates may be specified. These baud rates are used for speed matching with the device being attached to the PortMaster. Speeds are sequentially matched from the first baud rate (left side) through the third baud rate (right side). In Host Device mode, only the first baud rate is used.

- First baud - the first baud rate that PortMaster uses to synchronize with the attached device. Data rates from 300 bps to 115.2 Kbps (Kilobytes per second) are available. The default is 9600 bps.
- Second baud - a second baud rate that PortMaster can use to synchronize with the attached device. Data rates from 300 bps to 115.2 Kbps are available. The default is 9600 bps.
- Third baud - a third baud rate that PortMaster can use to synchronize with the attached device. Data rates from 300 bps to 115.2 Kbps are available. The default is 9600 bps.

Modem Control *(menu field)*

On or off may be selected. The default is "off". If "on" is selected the PortMaster uses the modem carrier detect line. The device will be idle until the carrier detect line is asserted. This value should be set to "on" when a modem has been attached. In addition, the modem should be set for "Normal" carrier detect.

Parity *(menu field)*

Even, odd, none, or strip may be selected. The default is "none". This value should be set to match the device being attached to the PortMaster. When even or odd is selected, 7 databits and 1 stop bit are assumed. When none is selected, 8 databits and 1 stop bit are assumed. When strip is selected, the parity bit will be removed from the data as it is received

by the PortMaster. See the "Extended Mode Parameters" section if another combination is required.

Login Message *(keyboard entry field)*

The message to be displayed to the user prior to the login prompt. Up to 240 characters can be in the message.

Extended Mode Parameters

In addition to the parameters described above in "Standard Mode Parameters", the following parameters may be set when Extended Mode is selected.

Flow Control *(menu field)*

PortMaster supports two types of flow control:

Xon/Xoff - This is a software flow control which is supported by most devices. By using the ASCII control characters DC1 and DC3 the PortMaster communicates with the attached device to start and stop the flow of data.

RTS/CTS - This is for devices where hardware flow control is required. When the PortMaster is able to receive data from the attached device, it raises Request to Send (RTS) on pin 4 of the RS-232 connector. Output from the PortMaster will only occur if the Clear to Send (CTS) modem line on pin 5 of the RS-232 connector is raised by the attached device.

Host *(menu field)*

The port can be configured to support three different ways of determining the host to establish a login session on:

Default - In this mode, the host entries entered in the global (network) edit screen are used for this port.

Prompt - In this mode, the user is given a host prompt (before the standard login prompt). The user then is required to enter a valid host name or internet address for a host on the network.

Specified - In this mode a primary host and up to two alternate hosts may be entered for this specific port. In this way each port can be independently assigned to a specific host computer. Ports which are configured for User Login will automatically switch to an alternate host if the Primary Host is unavailable (i.e. host 1 is down or network is unreachable). Login connections are attempted in the order in which the host names are entered. The first (or primary) host is required. The remaining hosts are optional and may be left blank.

Access Filter *(menu field)*

If the PortMaster is set to prompt the user for a host on this port, an optional access control filter can be specified. This filter is taken from the standard packet filter table described later in this chapter. After the user specifies a host, its address is compared against the designated filter. If the address is "permitted" by the filter, the user's connection will be allowed. If not, access will be denied. If the Access Override field is checked, and access has been denied, the user will be prompted for a username and password. The user's access filter from the User Table will then be used to determine if the user's private access filter provides sufficient additional capability to allow access to the designated host.

Pass-Thru Login *(menu field)*

If this field is enabled, users whose names do not match the local PortMaster Password Table entry will automatically be forwarded to the host specified in the "Host" field above. If this field is disabled, only users who are in the local users file or authenticated by RADIUS will be permitted to login.

Login Service *(menu field)*

The port can be configured to use one of four different network services for establishing login sessions.

PortMaster - This is the default service and can be used with any host workstation which has had a "Host Installation" performed from either **pminstall** or the install screen of **pmconsole**. This is the preferred

service because it makes the port operate like the serial ports physically installed in the workstation. It is the most efficient and highest performance service available.

Rlogin - This service is supported by a large number of mixed UNIX based computers. Therefore, where it is impractical to utilize the PortMaster service, Rlogin should be selected.

Telnet - This service is supported by a most TCP/IP implementations. Therefore, in a network where mixed hardware and operating systems will be used by this port, Telnet should be selected. The default TCP port number for telnet is 23, however an additional data entry field is provided to enter an alternate TCP port if required.

Netdata - This service can be used to create a virtual connection between this port and another serial port on a different PortMaster. The default TCP port number for netdata is 6000, however an additional data entry field is provided to enter an alternate TCP port if required. The serial port on the remote PortMaster must be configured as a Host Device Port using the same service and TCP port number.

Device Service *(menu field)*

The port can be configured to use one of four different network device services.

PortMaster - This is the default service and can be used with any host workstation which has had a "Host Installation" performed from either **pminstall** or the install screen of **pmconsole**. This is the preferred service because it makes the port operate like the serial ports physically installed in the workstation. When selected, the port is accessed through a /dev/tty device on the host workstation.

Rlogin - This service is supported by a large number of mixed UNIX based computers. Therefore, this service can be utilized to allow UNIX based workstations on the network to initiate an rlogin session to the PortMaster. Once the session is successfully established a host application is able to directly read and write data to the serial port. If multiple ports on the PortMaster are configured to use this service, it will

automatically create a "pool" of ports which can be accessed by other hosts. When all ports are in use, new users will be given a "Connection Refused" message.

Telnet - This service is supported by most TCP/IP implementations. Therefore, this service can be utilized to allow many different types of computers on the network to initiate a telnet session to the PortMaster. Once the session is successfully established, the host application will be able to directly read and write data to the serial port. If multiple ports on the PortMaster are configured to use this service, it will automatically create a "pool" of ports which can be accessed by other hosts. When all ports are in use, new users will be given a "Connection Refused" message. The default TCP port number for telnet is 23, however an additional data entry field is provided to enter an alternate TCP port if required.

Netdata - This service can be used for customized application programs that need a TCP connection directly to a serial port on the PortMaster. Programs which use the "socket" interface (or similar TCP interface) are provided with a direct data link to the PortMaster serial port. Port operating parameters are set with **pmconsole**. The application then opens a socket connection and immediately begins reading and writing to the PortMaster. No special option negotiation or protocol is required. The default TCP port number for netdata is 6000, though an additional field is provided to enter an alternate TCP port if required. If multiple ports on the PortMaster are configured to use this service with the same TCP port number, it will automatically create a "pool" of ports which can be accessed by other hosts. When all ports are in use, new users will be given a "Connection Refused" message.

Login Prompt *(keyboard entry field)*

This field allows the administrator to customize the login prompt the user will see. Any valid ASCII characters may be entered. The default is the Host Name followed by the word "login:". If "$hostname" is included in the login prompt, the active host name is substituted.

Autolog Name *(keyboard entry field)*

If this field is filled in the user will not receive the standard login prompt. Instead, the PortMaster will automatically initiate a session on the host as if the user had typed the Autolog Name in response to the login prompt.

Idle Timeout *(keyboard entry field)*

The idle timeout specifies how long the PortMaster should wait after the activity on the port stops before disconnecting the session. The idle timeout is specified in minutes and can be any value from 0 to 240. If set to 0, timeout is disabled.

Line Hangup *(menu field)*

If this field is enabled, the DTR signal on the RS-232 connector will be momentarily dropped to cause a modem or similar device to hangup after the termination of a user session. If disabled, DTR will not drop after the session terminates.

Dial Group *(keyboard entry field)*

This field is used by Dialnet for creating dial-out pools for serial network connections. When the PortMaster initiates a dial-out connection to a remote site, it will only allocate a port which is in the same dial group as has been specified for that location in the Location Table. Valid dial groups are numbered from 0 to 99. The default is 0.

Host Overrides *(menu field)*

The PortMaster allows host overrides to be selected for **Baud Rate**, **Parity**, **Databits**, and **Flow Control**. This feature allows the host to alter the active parameters via software control (i.e., system ioctl calls). Parameters which have a check mark in the box opposite them can be overridden. The default is that the host can only turn Xon/Xoff flow control on and off. This is useful for many Unix utilities like **uucp** and **tip**. If the parameter is not checked it cannot be overridden. In this case system requests to change these parameters will be ignored.

Hardwired Dialnet Parameters

The following parameters are only available for ports which are configured for Hardwired Dialnet connections.

Protocol *(menu field)*

This indicates which protocol to use for encapsulating packets. The options are:

PPP/IP - Use PPP with IP packet routing.

PPP/IPX - Use PPP with IPX packet routing.

PPP/IP/IPX - Use PPP with both IP and IPX packet routing.

SLIP - Use the Serial Line Internet Protocol.

MTU *(keyboard entry field)*

This is the Maximum Transmission Unit to be used for the interface. PPP connections can be set from 100-1500 octets and the remote computer can negotiate a smaller value than the setting entered. SLIP connections can be set from 100-1006. Maximum Transmission Unit defines the largest "frame" or "packet" which can be sent through this connection. If a packet is too large, it will be automatically fragmented. Setting this to smaller values can be useful for the TCP/IP protocol when using multi-line load balancing or for enhanced interactive performance while running large file transfers.

IP Destination *(keyboard entry field)*

The Internet Address or a valid host name of the system at the remote end of the point to point connection should be entered.

Netmask *(keyboard entry field)*

The netmask of the system at the remote end of the point to point connection should be entered.

IPX Network *(keyboard entry field)*

The IPX Network Address for the point to point connection should be

entered. This value must be in HEX format.

Routing *(menu field)*

This indicates whether the PortMaster should use the RIP protocol through the serial interface. The default is "Off". The following choices are available by using the "Next Choice" or "Pop-Up Menu" function keys:

On - The PortMaster will send RIP information to the remote device and will accept RIP information from the remote device.

Broadcast - The PortMaster will broadcast RIP information to the remote device.

Listen - The PortMaster will listen for RIP information from the remote device.

Off - The PortMaster will not send RIP information to the remote device and it will ignore all RIP messages it receives from the remote device.

MTU *(keyboard entry field)*

This is the Maximum Transmission Unit to be used for the interface. PPP connections can be set from 100-1500 octets and the remote computer can negotiate a smaller value than the setting entered. SLIP connections can be set from 100-1006. Maximum Transmission Unit defines the largest "frame" or "packet" which can be sent through this connection. If a packet is too large , it will be automatically fragmented. Setting this to smaller values can be useful when using multi-line load balancing or for enhanced interactive performance while running large file transfers.

Compression *(menu field)*

This indicates whether the PortMaster should use Van Jacobson TCP/IP header compression. This option can increase the performance of interactive TCP sessions if both sides of the link support this option. When configuring SLIP connections, both sides must be configured identically. When configuring PPP connections, if compression is enabled and the remote site doesn't support compression, the PortMaster

will dynamically disable this feature.

PPP Async Map *(keyboard entry field)*

The PPP protocol supports the escaping of non-printing ASCII in the data stream. Escaping means that specified characters will not be sent through the line, but instead will be replaced by a special set of characters which the remote site will interpret as the original character. The PPP Async Map is a bit-map of characters which should be escaped. The first (or zero) bit corresponds to the first ASCII character "NULL" and so on. Most environments should be set to zero to achieve maximum throughput.

Input Filter *(menu field)*

This menu item allows you to select from a list of all available input filters on the PortMaster. If specified, all packets received by the specified interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Packet Filters" later in this chapter.

Output Filter *(menu field)*

This menu item allows you to select from a list of all available output filters on the PortMaster. If specified, all packets being sent to the specified interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Packet Filters" later in this chapter.

Enabling Serial Port Parameters

If you would like to try a new port configuration without saving to the PortMaster permanent configuration:

- Select F2 (or Control-E) to view the Commands Menu.

- Select **APPLY** from this menu.
- Select **REMOTE RESET** from the Commands Menu.

The new port configuration will now be in effect until the PortMaster is rebooted or the parameters are changed again and applied.

If you want to save the new configuration in the permanent PortMaster configuration, select **SAVE** from the Commands Menu.

Setting the Parallel Port Configuration

This device type is always **Host Device**. For the parallel port to become active, assign a Host Device name (/dev/<device>) as described above under the heading "**Host Device**". In "**Extended Mode**" a specific host (other than the default) may be entered for the port. In addition, if a Device Service other than "**PortMaster**" is selected, the port becomes available as a network attached device in the same way as the serial ports described above.

Managing the IP Hosts Table

Each device attached to the Ethernet (which uses TCP/IP) is assigned a unique internet address. Internet addresses are four byte numerical values. To make it easier to remember these values, most systems on the network support a way of aliasing the internet address to some unique and easy to remember name. This is done on UNIX systems in the /etc/hosts file. The PortMaster also supports the same capability by maintaining a local hosts table.

The PortMaster hosts table should be used when any of the ports are set to prompt the user for a host name on the network. This table is then consulted to determine the correct internet address of the host.

If the host name specified by the user is not found in the hosts table, then the PortMaster will attempt to match the host name using either the Network Information Service (NIS), also known as "YP"; or DNS, the Domain Name Service. See the section "Global Configuration" for more information on setting the NIS or DNS server and domain.

To view or edit the PortMaster hosts table, log in to the PortMaster and select the "**Hosts**" command from the main console menu.

The hosts table stored in the PortMaster will be automatically retrieved into a working file on the workstation. **pmconsole** will then start an editor running to allow modifications to this file. As a default, **pmconsole** will run the "vi" editor. To choose an alternate editor, set the environment variable PM_EDITOR to the editor name.

Once edits or viewing have been completed, save the file and exit the editor. **pmconsole** will automatically download the file to the local hosts file in the PortMaster.

Managing the Users Table

The Users Table provides login security for users to establish login sessions or for incoming Dialnet network connections or for login terminal sessions.

Serial ports configured to accept login sessions initially prompt for a login user name. After receiving the login name, the PortMaster checks the name against the list of names in the local Users Table. If found, the PortMaster initiates password authentication of the user. If successfully validated (the password received matches the password stored in the Users Table, or on the RADIUS server) the PortMaster begins the session which has been defined for the user.

Four types of users can be created: **Network User/Normal**, **Network User/Dialback**, **Login User/Normal** and **Login User/Dialback**.

Network User/Normal users are allowed to immediately establish an active PPP or SL/IP connection to the network. **Network User/Dialback** users are disconnected by the PortMaster. The PortMaster then automatically dials to the user's remote modem using a predefined telephone number. **Login User/Normal** users are allowed to immediately begin an active session on a host on the network. **Login User/Dialback** users are disconnected by the PortMaster. The PortMaster then automatically dials to the user's remote modem using a predefined telephone number. This feature allows for enhanced security or for simple telephone charge-back.

If the login name does not match an entry in the Users Table and the port is configured to support **Pass-Thru Login** it automatically forwards the session to the designated host on the local network for password authentication. If your site is using the RADIUS authentication server the validation and login attributes are performed by the server.

To view or edit the PortMaster Users Table, log in to the PortMaster and select the "Tables" item from the main console menu. A pop-up menu will be displayed. Select "Users" from the menu.

The following screen will be displayed:

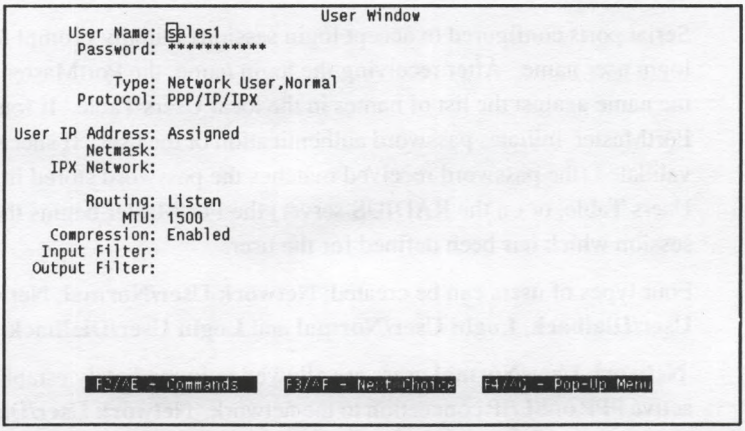


Figure 4-6. Users Screen

Upon entry, you will be in edit mode. This means that you can move around the screen with the arrow keys or by pressing <RETURN>. In addition, there is a set of function key labels across the bottom of the screen. Any of these function keys (or their associated Control characters) can be pressed at any time.

When "Control-E" is pressed, the function keys will be replaced by a menu of commands which can be executed. The available commands are:

- **Create** - Adds the currently displayed user to the PortMaster Users Table.
- **Modify** - Applies modifications to the user displayed on the Users Screen.
- **Delete** - Deletes the currently displayed user from the PortMaster Users Table.
- **Reset** - Clears the Users Screen to allow the entry of a new user.
- **Edit** - returns you to edit mode. The cursor moves back up onto the screen and the function key labels re-appear.

● **Done** - return to the PortMaster Console screen.

Login User Parameters

This screen displays the password table parameters and the current values. Some selections have menus. To use the menu, move your cursor to the field to be changed with the <RETURN> or arrow keys. Press the F4 function key (or Control-G) and a menu of choices will be displayed. You can rotate through the selections with the F3 function key (or Control-F). Other items can be edited directly from your keyboard by typing in new choices.

The Users table has 6 fields for each login user and 7 fields for dialback users. These fields are:

User Name *(menu and keyboard entry field)*

The login name of the user. The name can be up to 8 characters in length and is the user name expected to be provided at the "login:" prompt from the PortMaster.

Password *(keyboard entry field)*

The password for the user. This is a string of up to 16 ASCII characters.

Type *(menu field)*

All login users should be set to a type of "**Login User**". Login users can be set to "**Normal**" or "**Dialback**". Normal users will be allowed to immediately begin a login session after properly entering their user name and password. Dialback users will be disconnected by the PortMaster and then re-dialed at their pre-defined telephone number.

Host *(menu field)*

This field defines which host the user's session will be forwarded to. The three options and their meanings are:

Default - Connect the user to the defined host for this serial port. Consult the serial port edit screen for the defined host.

Prompt - Allow the user to select a host (either by IP address or name) to begin a login session.

Specified - Connect the user to the host specifically entered on the line below the Host selection. A valid hostname or IP address should be entered here.

Login Service *(menu field)*

The user can be set to use any of the available PortMaster Login Services. For a complete description of these services, consult the login service descriptions defined in the extended serial port parameters section of this manual.

Telephone No *(keyboard entry field)*

This field is only displayed for Dialback Login Users. The telephone number which should be dialed to reach the user's modem must be entered in this field. Dialback only supports modems with the Hayes "AT" command set.

Access Filter *(menu field)*

An optional access control filter can be specified for the user. This filter is taken from the standard packet filter table described later in this chapter. After the user specifies a host, its address is compared against the designated filter. If the address is "permitted" by the filter, the user's connection will be allowed. If not, access will be denied.

Network User Parameters

The Users Table is also used to maintain inbound network connections. The fields are similar to those used for Login Users, and there are some additional fields used which are not needed for Login Users. The complete set of fields is defined as follows:

User Name *(keyboard entry field)*

In the case of a Network User, this field is used as the ID of the inbound connection used in a "Chat" style script. For example, the login named used in a Location Table script would be the expected ID provided to the

PortMaster (see "Managing the Location Table" in the next section) .

Password *(keyboard entry field)*

The password for the inbound PPP or SL/IP user. This is a string of up to 16 ASCII characters.

Type *(menu field)*

Network users can be set to "**Normal**" or "**Dialback**". Normal network users will be allowed to immediately begin a PPP or SL/IP session after properly entering the correct ID and password. Dialback Network Users will be disconnected by the PortMaster and then re-dialed at their pre-defined telephone number.

Protocol *(menu field)*

This indicates which protocol to use for encapsulating packets. The options are:

PPP/IP - Use PPP with IP packet routing.

PPP/IPX - Use PPP with IPX packet routing.

PPP/IP/IPX - Use PPP with both IP and IPX packet routing.

SLIP - Use the Serial Line Internet Protocol.

User IP Address *(keyboard entry field)*

This is the IP address of the remote computer. Valid Address types are:

Specified - The specific IP address of the remote computer must be entered below the "Specified" label. The remote computer will only be allowed to operate with this IP address.

Assigned - The PortMaster will assign a temporary IP address for this session. This address will be retrieved from the pool of addresses being maintained by the PortMaster. See the Global Configuration screen for more information on Assigned Addresses.

Negotiated - This option is valid only for PPP sessions. The PortMaster will attempt to learn the IP address of the remote computer automatically.

Netmask *(keyboard entry field)*

The netmask of the system at the remote end of the dial-up connection should be entered.

IPX Network *(keyboard entry field)*

The IPX Network Address for the point to point connection should be entered. This value must be in HEX format.

Routing *(menu field)*

This indicates whether the PortMaster should use the RIP protocol through the serial interface. The default is "Off". The following choices are available by using the "Next Choice" or "Pop-Up Menu" function keys:

On - The PortMaster will send RIP information to the remote device and will accept RIP information from the remote device.

Broadcast - The PortMaster will broadcast RIP information to the remote device.

Listen - The PortMaster will listen for RIP information from the remote device.

Off - The PortMaster will not send RIP information to the remote device and it will ignore all RIP messages it receives from the remote device.

MTU *(keyboard entry field)*

This is the desired Maximum Transmission Unit to be used for the Interface. PPP connections can be set to values from 100-1500 octets and the remote computer can negotiate a smaller value than the setting entered. SLIP connections can be set to values from 100-1006. Maximum Transmission Unit defines the largest "frame" or "packet" which can be sent through this connection. If a packet is too large to fit, it will be automatically fragmented into smaller pieces by the PortMaster. Setting this to smaller (i.e., less than 300) values can be useful when using multi-line load balancing or for enhanced interactive performance while running concurrent file transfers.

Compression *(menu field)*

This indicates whether the PortMaster should use Van Jacobson TCP/IP header compression. This option can increase the performance of interactive TCP sessions if both sides of the link support this option. When configuring SLIP connections, both sides must be configured identically. When configuring PPP connections, if compression is enabled and the remote side doesn't support compression, the PortMaster will dynamically disable this feature.

Input Filter *(menu field)*

When specified as a Network User, this allows you to select from a list of all available input filters on the PortMaster. When specified, all packets received from the serial interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Packet Filters" toward the end of this chapter.

Output Filter *(menu field)*

When specified as a Network User, this allows you to select from a list of all available output filters on the PortMaster. When specified, packets being sent to the serial interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Packet Filters" later in this chapter.

Location Name *(keyboard entry field)*

This field is used for dialback network users, and is the name of the location stored in the PortMaster Location Table. After authenticating a Dialback Network User, the PortMaster will disconnect the active connection. It will then schedule an automatic dial to the specified location.

PPP Auto-Detect and PAP/CHAP negotiation

The PortMaster supports Auto-Detect PPP for use with the PAP and CHAP methods of login authentication. If the device at the remote end of the connection supports PAP or CHAP, when the login or host prompt

is provided by the PortMaster it will automatically detect PPP frames and the authentication will begin.

The CHAP challenge process (a practical example)

At the Corporate site is a PortMaster with the SNMP sysname of, for example, **pm1**. When a remote PortMaster establishes a connection and begins sending PPP frames, **pm1** becomes responsible for issuing a CHAP challenge. Inside that challenge is an ID string containing the name **pm1**. An entry for **pm1** is *required* in the PortMaster Users Table on the remote PortMaster.

When the remote PortMaster receives the challenge it does a lookup in its local Password Table. Finding the entry, it passes the password through MD5, and forms a response back to **pm1**. Contained within the response is an ID string containing the SNMP sysname of the remote PortMaster. **pm1** then looks in the Users Table for the ID of the remote PortMaster, and uses the password for that user to validate the CHAP response received from the remote PortMaster.

If the password comparison is successful, **pm1** will then send a "**CHAP successful**" message back to the remote PortMaster and the connection is complete. If the MD5 comparison fails, a "**CHAP failure**" message is sent to the remote PortMaster and the process repeats.

If the Corporate PortMaster wishes to use RADIUS to authenticate the remote PortMaster, the ID string and the password can be stored in the RADIUS users file on the RADIUS server. The password *must* be in clear text in order for the MD5 comparison to succeed.

Each PortMaster involved in this authentication must have an entry in its User Table which contains the SNMP sysname of the other PortMaster. The passwords must be identical.

Note: To clarify, the password for **pm1** is known as a *shared secret*, it is the same password used by the remote PortMaster. The name of the remote PortMaster and an identical password *must* be in the PortMaster Users Table on **pm1** or in the RADIUS users table on the RADIUS server for **pm1.**

For more information on the PortMaster authentication decision making tree, refer to Chapter 6, RADIUS.

Managing the Location Table

The Location Table is used for all dial-out network connections to remote locations. Each entry specifies a remote location, the operational parameters for that location, and information on how to establish a connection to that location.

To view or edit the PortMaster location table, log in to the PortMaster and select the "Tables" item from the main console menu and press <RETURN>. A pop-up menu will be displayed. Select "Locations" from the menu and press <RETURN>.

The following screen will be displayed:


```
                              Location Window
 Location Name: engineering     Type: On Demand        Protocol: PPP/IP/IPX
IP Destination: 149.198.196.1                          Netmask: 255.255.255.0
   IPX Network: 00000100
       Routing: On                                          MTU: 1500
  Input Filter:                                   Output Filter:
   Compression: Enabled                            Idle Timeout: 5
 Maximum Ports: 1          Group Number: 0          High Water: 0

  Dial Script:    Send: ATDT555-1212\r
                Expect: CONNECT
                  Send: \r
                Expect: login:
                  Send: corporate\r
                Expect: ssword:
                  Send: corp_password\r
                Expect: PPP
                  Send:
                Expect:
                  Send:
                Expect:

  F2/^E - Commands   F3/^F - Next Choice   F4/^G - Pop-Up Menu
```

Figure 4-8. Locations Screen

Upon entry, you will be in edit mode. This means that you can move around the screen with the arrow keys or by pressing <RETURN>. In addition, there is a set of function key labels across the bottom of the

screen. Any of these function keys (or their associated Control characters) can be pressed at any time. The function keys and their meanings are:

F2 or "Control-E" - Commands. When this key is pressed, the function keys will be replaced by a menu of commands which can be executed. The available commands are:

- **Create** - Creates a new location table entry based on the fields filled in on the location screen.
- **Modify** - Changes the parameters for the location specified in the Location Name field.
- **Delete** - Removes the selected location from the location table.
- **Reset** - Clears the fields on the location table window.
- **Edit** - Returns you to edit mode. The cursor moves back up onto the screen and the function key labels re-appear.
- **Done** - Return to the PortMaster Console screen.

F3 or "Control-F" - Next Choice. When this key is pressed, and the cursor is on a menu field, the next available choice for that menu will be displayed.

F4 or "Control-G" - Pop-up Menu. When this key is pressed, and the cursor is on a menu field, a menu of available choices will be displayed.

To create a new location, simply fill in all of the fields in the location screen and select the F2 (Control-E) function key. Select "**Create**" from the menu.

To modify an existing entry, first select that entry from the pop-up menu on the Location Name field. Change the necessary parameters. Then select "**Modify**" from the Commands menu.

To delete an existing entry, first select that entry from the pop-up menu on the Location Name field. Then select "**Delete**" from the Commands menu.

Location Table Parameters

These are the parameters which can be selected and edited from this

screen:

Location Name *(menu and data entry field)*

The name of the remote location. This can be any 12 character name to identify the remote location. It is generally not the name of a single system, but rather an identifier which represents the entire location (i.e., the city or the company name at that location).

Type *(menu field)*

On Demand - This selection notifies the PortMaster to dial and establish a connection to the remote location only when packets are queued for that location. In this mode the PortMaster creates a network interface and the appropriate routing information to notify the attached local area network of the connectivity to the remote site. This is done even though there may not be an actual physical connection to that site at the time.

Continuous - This selection notifies the PortMaster to always keep the dial-up connection to the remote site active. If the telephone line is lost, the PortMaster will automatically initiate a re-dial to that location.

Manual - This selection notifies the PortMaster to only dial to the remote location when an operator requests the connection. This can be done from the **pmconsole** Dialer Screen or it can be invoked from the "**pmdial**" program installed on one of the workstations on the network. This also allows connections to be scheduled by using the UNIX cron scheduler to call pmdial.

Note: When switching a location from Manual to On-demand make sure the dial-out connection has been closed (reset the serial port) before updating the location table.

Protocol *(menu field)*

This indicates which protocol to use for encapsulating packets. The options are:

PPP/IP - Use PPP with IP packet routing.

PPP/IPX - Use PPP with IPX packet routing.

PPP/IP/IPX - Use PPP with both IP and IPX packet routing.

SLIP - Use the Serial Line Internet Protocol.

IP Destination *(data entry field)*

For SLIP connections, the IP Address or a valid host name of the system at the remote end of the dial-up connection should be entered.

For PPP connections, the Destination can be negotiated. In this mode, the PortMaster can automatically learn the IP address of the remote system. Enter the word "Negotiated" in this field to enable this feature. This should only be used for manual or continuous connections. On-Demand locations must use a specified address.

Netmask *(data entry field)*

The netmask of the system at the remote end of the dial-up connection should be entered.

IPX Network *(keyboard entry field)*

The IPX Network Address for the point to point connection should be entered. This value must be in HEX format.

Routing *(menu field)*

This indicates whether the PortMaster should use the RIP protocol through the serial interface. The default is "Off". The following choices are available by using the "Next Choice" or "Pop-Up Menu" function keys:

On - The PortMaster will send RIP information to the remote device and will accept RIP information from the remote device.

Broadcast - The PortMaster will broadcast RIP information to the remote device.

Listen - The PortMaster will listen for RIP information from the remote device.

Off - The PortMaster will not send RIP information to the remote device

and it will ignore all RIP messages it receives from the remote device.

MTU *(data entry field)*

This is the desired Maximum Transmission Unit to be used for the Interface. PPP connections can be set to values from 100-1500 octets and the remote computer can negotiate a smaller value than the setting entered. SLIP connections can be set to values from 100-1006. Maximum Transmission Unit defines the largest "frame" or "packet" which can be sent through this connection. If a packet is too large to fit, it will be fragmented into smaller pieces by the PortMaster. Setting this to smaller (i.e., less than 300) values can be useful when using multi-line load balancing or for enhanced interactive performance while running concurrent file transfers.

Input Filter *(menu field)*

This field allows you to select from a list of all available input filters on the PortMaster. When specified, all packets received from the serial interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Packet Filters" toward the end of this chapter.

Output Filter *(menu field)*

This field allows you to select from a list of all available output filters on the PortMaster. When specified, packets being sent to the serial interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Packet Filters" later in this chapter.

Compression *(menu field)*

This indicates whether the PortMaster should use Van Jacobson TCP/IP header compression. This option can increase the performance of interactive TCP sessions if both sides of the link support this option. When configuring SLIP connections, both sides must be configured identically. When configuring PPP connections, if compression is enabled and the remote side does not support compression, the PortMaster will dynamically disable this feature.

Idle Timeout *(data entry field)*

For Manual and On-Demand type locations this specifies the number of minutes the line should be idle (no network traffic to the remote site) before disconnecting the telephone connection.

Maximum Ports *(data entry field)*

The number of dial-out ports the PortMaster can use for this network connection. If 0 is selected dialing to this location will be disabled. If more than 1 is selected the PortMaster will use the "High Water Mark" to decide when to open and dial additional lines. If more than one line is open to the remote location the PortMaster will automatically use load balancing to achieve the maximum throughput of all lines combined. If multiple lines are open the "Idle Timeout" value will be used to decide when to disconnect unneeded lines.

High Water Mark *(data entry field)*

The number of bytes of queued traffic required to open an additional dial-out line to the remote site. This is only used when the "Maximum Ports" value is greater than 1 and there are available modems on the PortMaster. Setting a very small number causes the PortMaster to quickly use all of the ports specified in "Maximum Ports". Generally, interactive terminal traffic has no more than a few hundred bytes queued at any one time. However, file transfers (i.e., ftp) will queue several thousand bytes. These size differences should be used when deciding what number to use for the High Water Mark.

Group Number *(data entry field)*

The modem pool group to which this location is assigned. Only modem ports which are configured with this Group Number will be available for dial-out to this location. This can be used to reserve modems for dial-up to specific locations or to differentiate different types of modems which would be compatible with the remote location.

Dial Command Script *(data entry field)*

This script is used to issue commands to the modem (or other similar equipment) to dial the correct number and establish the link. In addition, this script is used for authentication (password security) at the remote site. Each "Send" string is issued out of the PortMaster serial port to the modem or remote computer. Each "Expect" string is used by the PortMaster to verify that the previous "Send" string was properly received by the modem or remote computer and the PortMaster should transmit the next "Send" string.

Send - This string can be up 30 characters in length. Any printing ASCII character can be placed in this string. In addition, the following special characters are available:

\r - This is replaced by the ASCII carriage return character.

\n - This is replaced by the ASCII line feed character.

\0XX - This is replaced by the octal digit specified in the XX.

\\ - This is replaced by the single backslash (\) character.

Generally Send strings would end with the "\r" character.

Expect - This string can be up to 30 characters in length. Any printing ASCII character can be placed in this string. In addition, any of the special characters from above can be used. Generally, a valid reply can be determined by checking for the last word received from the remote system. For example if the remote system is prompting for a login id, it may issued the string:

```
Please enter your login:
```

The Expect string in the Dial Command Script could simple look for "login:".

It is recommended that the last entry in the Dial Command Script be an Expect string which indicates that the remote location is ready to begin receiving network packets. This is used to activate the data link protocol coming from the PortMaster. When connecting to a remote PortMaster the final reply string to look for should be "SL/IP" for SLIP connections and "PPP" for PPP connections. For other products, consult that vendors users manual.

The following Dial Command Script is an example of how to establish a connection between two PortMasters which have modems supporting the "AT" dial command syntax:

```
  Send: ATDT18005551212\r
Expect: CONNECT
  Send: \r
Expect: login:
  Send: my_location_name\r
Expect: ssword:
  Send: my_password\r
Expect: PPP
```

The "18005551212" would be replaced by the actual telephone number of the remote modem. "my_location_name" would be replaced by the actual user name for your location. "my_password" would be replaced by the actual password set up at the remote site which corresponds to the user name.

PPP CHAP authentication

The PortMaster supports CHAP method of login authentication. If there is a PortMaster at the remote end of the connection, it will immediately begin the PPP negotiation once the connections is established. The PortMaster supports login authentication through CHAP protocol from the remote device; when it receives the challenge, it uses the id string (the remote system name) contained in that challenge to locate an entry in the local User Table. It will then use the user it finds to construct the correct authentication response to the challenge. Refer to the detailed discussion on PAP and CHAP authentication earlier in this chapter.

Dialing Out to Remote Locations

On-demand or Continuous dial-out locations automatically initiate dialing to a remote location. Manual connections require a system administrator or a scheduler to initiate dial-out connections. **pmconsole** provides a facility for the system administrator to initiate the dial-out operation and if necessary to monitor the progress of the dial-out operation.

When setting up a new On-demand location it is recommended to first set up the location as a manual dial-out site for testing purposes and then later switch the location type to On-demand.

Note: When switching a location from Manual to On-demand, make sure the dial-out connection has been closed (reset the serial port) before updating the location table.

To initiate dial-out connections via a scheduler (i.e., cron in UNIX systems) or from a UNIX command line prompt see the "**pmdial**" command in the UNIX Utilities section of this manual.

To dial to a remote location from **pmconsole**, select the "View" button from the main console with your right mouse button. A pop-up menu will be displayed. Select "Dialer" from the menu. The screen in Figure 4-9 will be displayed.

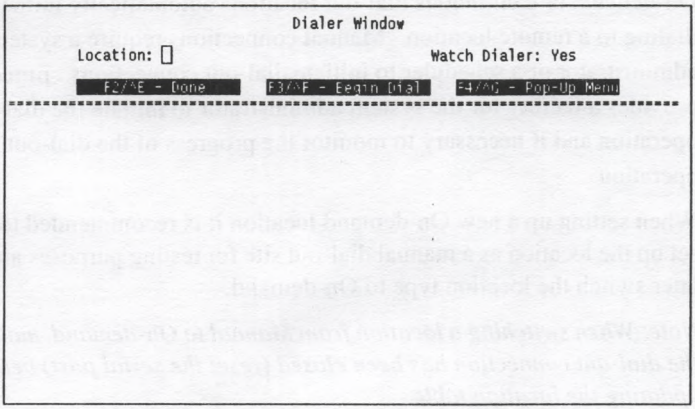


Figure 4-9. Dialer Screen

Location

This is the location to dial. This field is filled in by selecting one of the locations from the pop-up menu with the arrow keys.

Watch Dialer

The F-key labels (or control characters) are used to access the available functions. These are:

F4 (or Control-G) - Call the pop-up menu.

F3 (or Control-F) - Begin dialing the specified location.

F2 (or Control-E) - Done.

To begin dialing to a remote location hit F3 or enter "Control-F". Then select "**Yes**" or "**No**" as the monitoring option.

If "**Yes**" was selected in the Watch Dialer field, the message window will show the location being dialed and the modem port being used. It will then show the execution of the Dial Command Script. The "sendthem" message shows the exact string of characters being sent out the serial port to the modem or remote system enclosed in parentheses. The

"expect" message shows the response string the PortMaster is expecting as a reply enclosed in parentheses. Immediately following the "expect" string are the characters actually being received by the PortMaster from the modem or remote system. When the PortMaster successfully receives the string is is searching for, it will display ":got it" followed by the next send message.

No - Causes the PortMaster to start dialing the location and immediately returns control to **pmconsole** for another operation.

If the dial script completes successfully, the message "Connection Succeeded" will be displayed. Otherwise, after timing out, the message "Connection Failed" will be displayed.

Managing the Routes Table

The PortMaster Routes table is used when static network routes are required. Static routes are required when the user chooses not to run the Routing Information Protocol (RIP) on the PortMaster, or when hosts or networks attached to the PortMaster do not have the ability to run the RIP protocol. There are two static routing tables maintained by the PortMaster. One is for IP and the other is for IPX. IP routes contain three entries:

Destination - This is the host or network to which the PortMaster will be required to send packets.

Gateway - This is the directly connected host through which packets should be forwarded to reach the above destination.

Metric - This is a metric representing the cost of sending the packet through the above gateway. Generally metric is the HOP count to the remote network. The number of gateways the packet must cross to reach its destination.

IPX routes contain four entries:

Destination - This is the IPX network to which the PortMaster will be required to send packets.

Gateway - This is the directly connected host through which packets should be forwarded to reach the above destination. It is represented by the combination of network number and node address separated by a colon (i.e., 00001234:00AABBCCDDEE).

Metric - This is a metric representing the cost of sending the packet through the above gateway. Generally metric is the HOP count to the remote network. The number of gateways the packet must cross to reach its destination.

Ticks - This is a number representing the time it takes to send the packet to its destination network in 50ms increments.

To view or edit the PortMaster routes table, log in to the PortMaster and select the "**Tables**" item from the main console menu. A pop-up menu will be displayed. Select "**Routes**" from the menu. A pop-up menu will be displayed. Select the correct routing table from the menu (IP or IPX).

The routes table stored in the PortMaster will be automatically retrieved into a working file on the host. **pmconsole** will then start an editor to allow modifying the file. **pmconsole** starts the "vi" editor by default, or will start an editor defined in the environment variable PM_EDITOR.

Once editing or viewing has been completed, save the file and exit the editor. **pmconsole** will automatically download the file to the local routes file in the PortMaster.

Packet Filters

Packet filters are used primarily as a security mechanism in networks which cross organizational or corporate boundaries. They are useful in limiting certain kinds of inter-network communications by specifically permitting or denying packets through network interfaces. By designing appropriate filters, systems administrators can control access to specific computers, networks, and network services.

Packet filters require the analysis of the header information contained in each packet sent or received through a network interface. This header information is evaluated against a set of rules which allow the packet to pass freely through the interface (and on to its destination in the network) or cause the packet to be discarded without forwarding.

The Livingston packet filtering mechanism is designed around two primary objectives. First, maximum flexibility is required to allow the administrator to achieve the desired results without compromising security. Second, efficiency is desirable to maximize network performance. Specific features which support these objectives are:

- **Input** and **Output** Filters - Each interface can be assigned both an input-packet filter and an output-packet filter. This is especially useful in PortMasters with more than two network interfaces and it simplifies the design task. The administrator can evaluate each interface for its destination and the mix of inbound and outbound traffic desired for the interface. This capability also has the potential to decrease the number of rules contained in the filter because fewer network numbers need to be included.

- **Source and Destination Address Filtering** - Both source and destination addresses are evaluated in the rule list. Also, the number of significant bits to use in IP address comparisons can be set. This allows filtering based on specific hosts, subnets, or network numbers.

- **Protocol Filtering** - Specific protocols can be handled separately in the packet filters. These include IPX and TCP, UDP, and ICMP for IP.

- **Source and Destination Port Filtering** - The source and destination port numbers can be used in the rule set to control availability of specific network services. This includes evaluation based upon whether the port number is less than, equal to, or greater than a specific value.

- **Established Session Filtering** - The status of TCP connections can be used as part of the rule set. This allows users in a network to open connections to external networks without allowing external users access to the local network.

- **Unlimited Number of Rules** - Each filter can have a large number of rules specified. This is only limited by available memory within the router.

- **Simple Rule Creation** - The command syntax for creating specific rules allows the administrator to specify only as much information as is necessary to specify the rule. For example if the rule is not based upon specific source and destination IP address, these addresses can be omitted from the specification of the rule.

- **In-line Rule Processing** - Rules are processed in the order in which they are specified in the rule set. This eliminates ambiguity about how a specific packet would be handled, and allows more flexibility in creating a packet filter.

Filter Organization

The PortMaster maintains a table of packet filters in its permanent configuration memory. These filters can be created or modified at any time and are independent of any active packet filters. Each filter is assigned a name of up to 15 characters in length. Each packet filter has three sets of rules. These are IP rules, IPX rules and SAP rules. Each

rule set is made up of a list of rules which are numbered starting at 1. A packet filter when initially created contains no rules.

IP and IPX packet filters are "attached" to interfaces as either input or output filters. SAP filters are attached only as output filters. For serial interfaces, the packet filter is enabled when it transitions to the UP state (i.e., after a reset on the port). The Ethernet interface filter is enabled as soon as the name of the input or output filter is specified.

Managing the Filter Table

From the "**Tables**" pop-up menu, select "**Filters**". The screen shown in Figure 4-10 will appear.

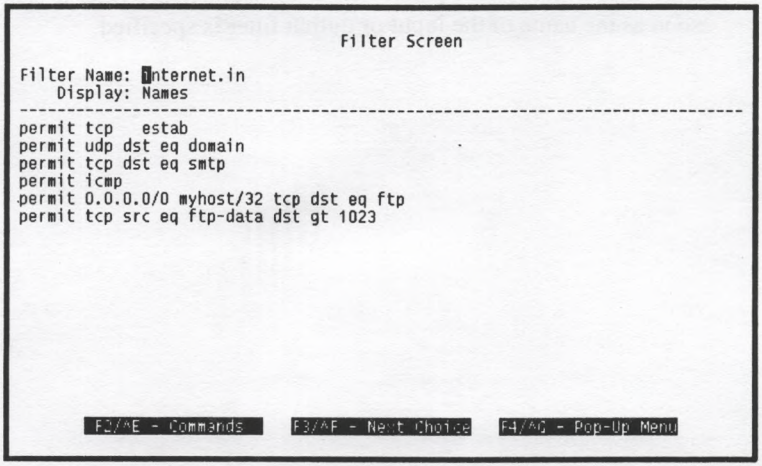

Filter Screen
Filter Name: Internet.in
Display: Names
permit tcp estab
permit udp dst eq domain
permit tcp dst eq smtp
permit icmp
permit 0.0.0.0/0 myhost/32 tcp dst eq ftp
permit tcp src eq ftp-data dst gt 1023
F2/^E - Commands
F3/^F - Next Choice
F4/^C - Pop-Up Menu

Figure 4-10 Filter Screen

Upon entry, you will be in edit mode. This means that you can move around the screen with the arrow keys or by pressing <RETURN>. In addition, there is a set of function key labels across the bottom of the screen. Any of these function keys (or their associated Control characters) can be pressed at any time.

Entering "Control-E" will cause the function keys to be replaced by a menu of commands which can be executed. The available commands are:

- **Create** - Adds the currently displayed filter to the PortMaster Filter Table.
- **Modify** - Applies modifications to the filter displayed on the Filter Screen.
- **Delete** - Deletes the currently displayed filter from the PortMaster Filter Table.

- **Reset** - Clears the Filter Screen to allow the entry of a new filter.
- **Edit** - returns you to edit mode. The cursor moves back up onto the screen and the function key labels re-appear.
- **Done** - Removes the Filter Screen from the display.

Filter Name

This field displays the name of the current packet filter being edited or the name of the new filter being created. Selecting a name from the pop-up list will fill in the Filter Name.

Display

The display field can be changed at any time and is only used for IP filters. When set to "Names", the rules will convert IP address to host names and port numbers to service names. When set to "Numbers", IP addresses will be displayed in standard dot notation and services will be displayed numerically.

Rule Set

The Rule Set should be set to the type of filter which requires editing. After completing an edit, the rule set should be saved before beginning the edit of a new filter or a different rule set in the same filter.

Edit

Upon entering the Edit area of the screen the F3 (or "Control-F" key) places you into your editor of choice (the PM_EDITOR environment variable) which will allow you to edit the Filter. Exiting the editor places you back into the Edit area and refreshes the area to include the information added from within your editor.

Filter Rule Syntax

The rule set for the filter is entered on the screen or from within an editor as described above. Entries can be inserted, deleted, and moved around within this screen. Because packets are evaluated starting at the first rule, the most common packets which will be handled by the router

should be specified first. As soon as a packet matches a rule the action specified by the rule will be immediately taken. If the packet does not match any rule, the action will be to deny the packet from traveling through the interface.

IP Rules

The syntax for specifying an IP rule is:

action [source_address/bits destination_address/bits] protocol options

Actions are specified as the first entry in a rule. Valid actions are:
permit - Permit the packet to pass freely through the interface.
deny - Stop the packet from traveling through the interface.

Source_address/bits - specify the comparison with the source IP Address contained in the packet. The number of bits (0-32) are first extracted from the IP Address in the packet (i.e., if 24 bits is specified, a packet with the source address of 192.9.200.1 would become 192.9.200.0 since 24 bits are used to represent the first 3 bytes of the address). The most common bit counts would be:

0 - To match packets with any source IP Address.
16 - To look at only the network number of a class B IP Address.
24 - To look at only the network number of a class C IP Address.
32 - To look at the entire IP Address.

The resulting value is then compared with the specific source address.

Destination_address/bits - specify the comparison with the destination IP Address contained in the packet. The number of bits (0-32) are first extracted from the IP Address in the packet. The resulting value is then compared with the specific destination address.

Protocol - The protocol of the packet may be specified. Valid values are TCP, UDP or ICMP.

Options - Each protocol supports a specific list of options:

TCP - This type of rule supports filtering on source and destination port numbers as well as the established state of the connection. The syntax

for TCP options is:

[src eq|gt|lt port_number] [dst eq|gt|lt port_number] [estab]

Where:

src - indicates a comparison should be made with the source TCP port number.

dst - indicates a comparison should be made with the destination TCP port number.

eq - indicates that the port number in the packet should be tested to see if it is equal to the port number specified in the rule.

gt - indicates the the port number in the packet should be tested to see if it is greater than the port number specified in the rule.

lt - indicates that the port number in the packet should be tested to see if it is less than the port number specified in the rule.

estab - indicates that the packet should be tested to see if it is for an established TCP network connection. If this key word is specified packets being sent to establish new TCP connections would not match this rule.

UDP - This type of rule supports filtering on source and destination port numbers. The syntax for UDP options is:

[src eq|gt|lt port_number] [dst eq|gt|lt port_number]

Where:

src - indicates a comparison should be made with the source UDP port number.

dst - indicates a comparison should be made with the destination UDP port number.

eq - indicates that the port number in the packet should be tested to see if it is equal to the port number specified in the rule.

gt - indicates the the port number in the packet should be tested to see if it is greater than the port number specified in the rule.

lt - indicates that the port number in the packet should be tested to see if it is less than the port number specified in the rule.

ICMP - This type of rule supports filtering on type of ICMP message. The syntax for ICMP options is:

[src eq icmp_message_type]

Where a comparison is made with the ICMP message type contained in the packet.

IPX Rules

The syntax for specifying an IPX rule is:

action [keyword value] [keyword value] ....

Actions are specified as the first entry in a rule. Valid actions are:

permit - Permit the packet to pass freely through the interface.

deny - Stop the packet from traveling through the interface.

Valid keywords are:

srcnet - Specifies the comparison with the source IPX Network Address contained in the packet. This value should be specified in HEX format.

dstnet - Specifies the comparison with the destination IPX Network Address contained in the packet. This value should be specified in HEX format.

srchost - Specifies the comparison with the source IPX Node Address contained in the packet. This value should be specified in HEX format.

dsthost - Specifies the comparison with the destination IPX Node Address contained in the packet. This value should be specified in HEX format.

srcsocket - Specifies the comparison with the source IPX socket number contained in the packet. A second keyword indicating the type of comparison must be specified. Valid comparison types are "equal", "lessthan" or "greaterthan". Following the comparison keyword, a numeric value should be specified in HEX format.

dstsocket - Specifies the comparison with the destination IPX socket

number contained in the packet. A second keyword indicating the type of comparison must be specified. Valid comparison types are "equal", "lessthan" or "greaterthan". Following the comparison keyword, a numeric value should be specified in HEX format

SAP Rules

The syntax for specifying a SAP rule is:

action [keyword value] [keyword value] ....

Actions are specified as the first entry in a rule. Valid actions are:

permit - Permit the service to be advertised on this interface.

deny - Stop the service from being advertised on the interface.

Valid keywords are:

server - Specifies the comparison with the name of the server which is advertising its service.

network - Specifies the comparison with the server's IPX Network Address. This value should be specified in HEX format.

host - Specifies the comparison with the server's IPX Node Address. This value should be specified in HEX format.

socket - Specifies the comparison with the server's IPX socket number . A second keyword indicating the type of comparison must be specified. Valid comparison types are "equal", "lessthan" or "greaterthan". Following the comparison keyword, a numeric value should be specified in HEX format.

Filter Table Example

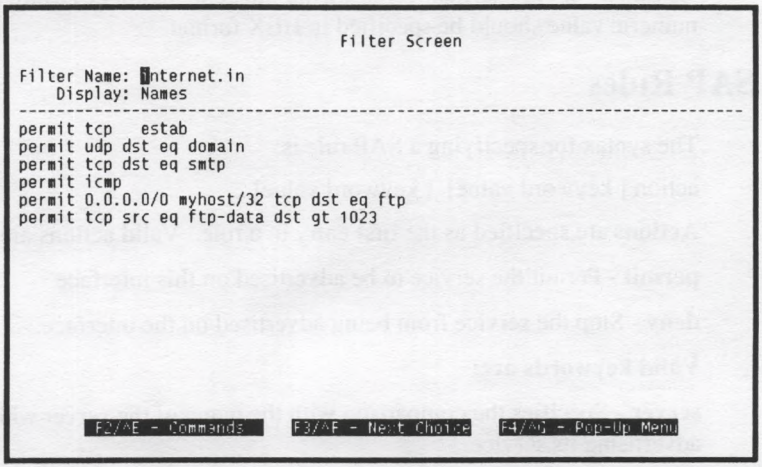

Filter Screen
Filter Name: Internet.in
Display: Names
permit tcp estab
permit udp dst eq domain
permit tcp dst eq smtp
permit icmp
permit 0.0.0.0/0 myhost/32 tcp dst eq ftp
permit tcp src eq ftp-data dst gt 1023
F2/^E - Commands
F3/^F - Next Choice
F4/^G - Pop-Up Menu

Figure 4-11. Filter Example Screen

In figure 4-11, Rule 1 says we permit established connections. Therefore any TCP connection which was originated to a foreign host will be permitted.

Rule 2 says we permit udp Domain Name Service packets from any foreign host.

Rule 3 says we permit smtp (sendmail) packets.

Rule 4 says we permit ping packets.

Rule 5 says we permit ftp from any foreign host but only to "myhost".

Rule 6 is used with rule 5 to allow the data portion of the ftp traffic to be forwarded correctly..

For examples of other filter rules, refer to the "Command Prompt Interface" section of this manual.

Configuring SNMP

The PortMaster provides support for the Simple Network Management Protocol (SNMP) for getting and setting network management data. Specifically it provides the industry standard MIB-2 variables. These variables are fully described in the Livingston MIB distributed with the standard Livingston software. This MIB along with configuration files for various network management packages can be found in the "snmp" directory of the software. **pmconsole** provides a screen for configuring and enabling the SNMP facilities of the PortMaster. The SNMP edit screen can be displayed by using the "Edit" pop-up menu from the main console screen. After selecting "SNMP" from this menu, the following screen will be displayed:

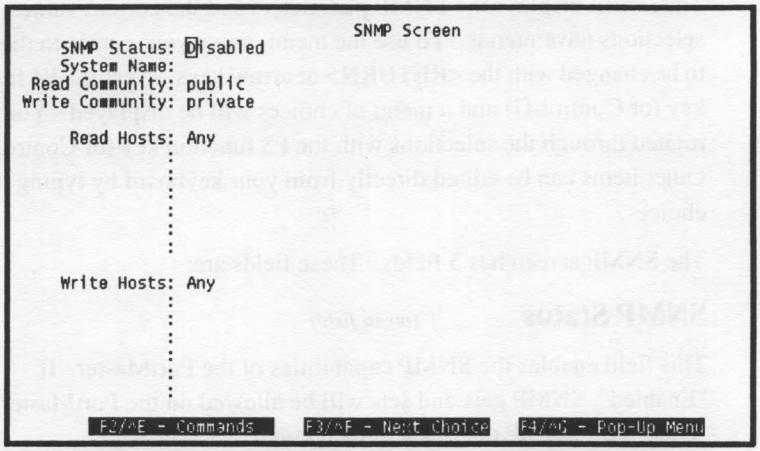


Figure 4-12. SNMP Screen

Upon entry, you will be in edit mode. This means that you can move around the screen with the arrow keys or by pressing <RETURN>. In addition, there is a set of function key labels across the bottom of the screen. Any of these function keys (or their associated Control characters) can be pressed at any time.

When F2 (or "Control-E") key is pressed, the function key is replaced by a menu of commands which can be executed. The available commands are:

- Save - Stores the currently displayed values to the non-volatile storage in the PortMaster.
- Reset - Sets all values to their factory default configuration.
- Edit - returns you to edit mode. The cursor moves back up onto the screen and the function key labels re-appear.
- Done - return to the PortMaster Console screen.

SNMP Parameters

The screen displays the SNMP parameters and the current values. Some selections have menus. To use the menu, move your cursor to the field to be changed with the <RETURN> or arrow keys. Press the F4 function key (or Control-G) and a menu of choices will be displayed. You can rotated through the selections with the F3 function key (or Control-F). Other items can be edited directly from your keyboard by typing in new choices.

The SNMP screen has 5 fields. These fields are:

SNMP Status *(menu field)*

This field enables the SNMP capabilities of the PortMaster. If "Enabled", SNMP gets and sets will be allowed on the PortMaster. If "Disabled", SNMP queries will be ignored.

System Name *(keyboard entry field)*

This field sets the global SNMP system name. It is used as a system identifier independent of protocols. In addition, it is used as the system identifier in PPP PAP and CHAP requests.

Read Community *(keyboard entry field)*

The SNMP read community is used to segregate administrative manage-

ment communities. This should be set to match the read community setting of your SNMP management software. The default is "public".

Read Hosts *(menu field)*

For security purposes, the hosts which are allowed to perform SNMP gets can be set on the PortMaster. The options are:

Any - All hosts using the correct read community will be allowed to retrieve SNMP data from the PortMaster.

None - No SNMP reads will be responded to by the PortMaster.

Specified - A specific list of hosts can perform SNMP gets from the PortMaster. A set of input fields will be displayed on the screen for the entry of a list of hosts.

Write Community *(keyboard entry field)*

The SNMP write community is generally used to segregate administrative management communities. This should be set to match the write community setting of your SNMP management software. The default is "private".

Write Hosts *(menu field)*

For security purposes, the hosts which are allowed to perform SNMP sets can be set on the PortMaster. The options are:

Any - All hosts using the correct write community will be allowed to set SNMP data on the PortMaster.

None - No SNMP writes will be allowed by the PortMaster.

Specified - A specific list of hosts can perform SNMP sets on the PortMaster. A set of input fields will be displayed on the screen for the entry of a list of hosts.

RADIUS

The PortMaster supports RADIUS (Remote Authentication Dial In User Service). This service supports authentication of users and remote PortMasters from a centrally managed database maintained on an authentication server somewhere on the network. For information on implementing a RADIUS authentication server, see Chapter 6. **pmconsole** allows the administrator to configure the PortMaster as a RADIUS client. In this configuration, the PortMaster will first consult its local Password Table (See Password Table Maintenance earlier in this chapter), it will then consult the RADIUS server if the user is not locally defined.

From the PortMaster Console Screen, select the Edit pop-up menu and select **RADIUS**. The following screen will be displayed:

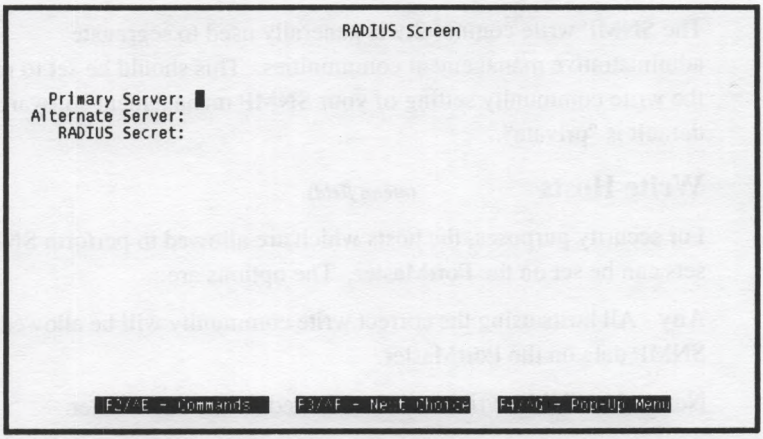


Figure 4-13. RADIUS Screen

Primary Server - Enter the hostname or the IP address of the Primary Authentication Server.

Alternate Server - Enter the name of the Secondary Authentication Server.

RADIUS Secret - enter the secret used to encrypt users passwords and for verification of the responding RADIUS server. Note that when entering the RADIUS secret from **pmconsole** it is passed over the network in clear text. Alternately this secret may be entered using the command line interface directly through the serial port on the PortMaster.

Note: For information on the RADIUS server refer to Chapter Six.

Monitoring the PortMaster

pmconsole allows the monitoring of traffic, errors, and sessions through the serial and parallel ports, as well as monitoring statistics for each of its network interfaces. The View command on the main console screen allows selection of either "Ports", "Netstats", or "Sessions".

Port View Screen

From the PortMaster Console screen, select the VIEW command. Then select "Ports" from the menu. A screen similar to Figure 4-14 will be displayed.

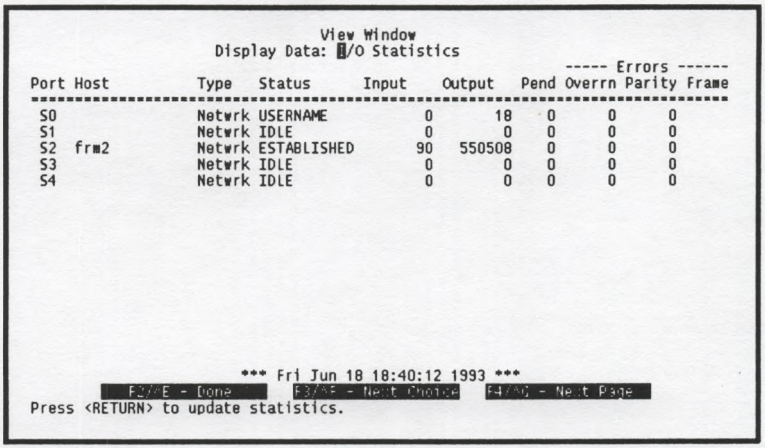

View Window
Display Data: I/O Statistics
----- Errors ------
Port Host Type Status Input Output Pend Overrn Parity Frame
S0 Netwrk USERNAME 0 18 0 0 0
S1 Netwrk IDLE 0 0 0 0 0
S2 frm2 Netwrk ESTABLISHED 90 550508 0 0 0
S3 Netwrk IDLE 0 0 0 0 0
S4 Netwrk IDLE 0 0 0 0 0
*** Fri Jun 18 18:40:12 1993 ***
F2/^E - Done
F3/^F - Next Choice
F4/^G - Next Page
Press <RETURN> to update statistics.

Figure 4-14. View Ports Screen

This screen allows you to view the configuration and Status of each port. These values are refreshed each time you press the <RETURN> key.

Three sets of data can be displayed in the view screen. These are the "**Active Configuration**", "**I/O Statistics**" and "**Sessions**". All three display the port, the port type, and the current status of the port.

When "**Active Configuration**" is selected (using F3 or F4 function keys), the screen displays data communications parameters such as baud rate, databits and parity.

When "**I/O Statistics**" is selected the screen displays input and output information. There are three columns labeled: Input, Output, and Pending. These relate to the number of bytes transferred in or out the port and the number of bytes in the PortMaster output buffer which are pending to be output. There are also three error counts displayed: Overrun, Parity and Framing errors.

When "**Sessions**" is selected the screen displays active users (if the session was started by a dial-up process) the direction in which the connection was started, the time since the active session was started, how long the port has been idle, and the idle timeout if one has been set.

Network Statistics

After selecting "Netstats" from the VIEW menu, the screen in Figure 4-15 will be displayed.

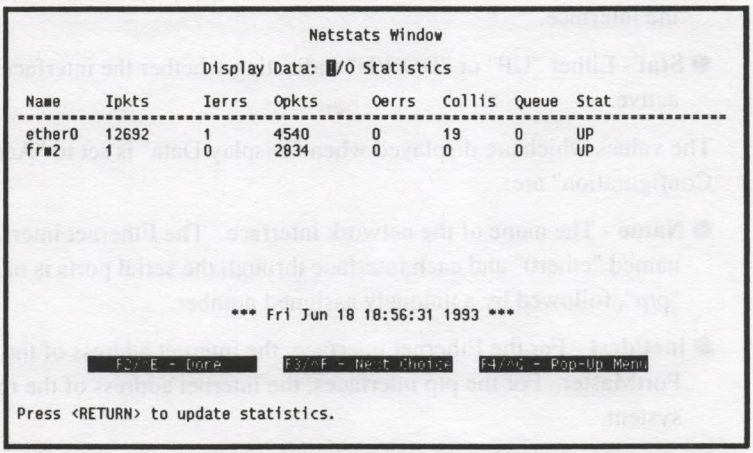

Netstats Window
Display Data: I/O Statistics
Name Ipkts Ierrs Opkts Oerrs Collis Queue Stat
ether0 12692 1 4540 0 19 0 UP
frm2 1 0 2834 0 0 0 UP
*** Fri Jun 18 18:56:31 1993 ***
F2/^E - Done
F3/^F - Next Choice
F4/^G - Pop-Up Menu
Press <RETURN> to update statistics.

Figure 4-15. Netstats Screen

This screen allows you to view the Status of each network interface in the PortMaster. These values are refreshed each time you press <RETURN>.

The values which are displayed when "Display Data" is set to "I/O Statistics" are:

- **Name** - The name of the network interface. The Ethernet interface is named "ether0" and each interface through the serial ports is named "ptp", followed by a uniquely assigned number.
- **Ipkts** - The number of input packets received by the interface.
- **Ierrs** - The number of input packets received by the interface which were dropped due to errors.
- **Opkts** - The number of output packets sent by the interface.
- **Oerrs** - The number of output packets which were not sent by the interface due to errors.
- **Collis** - The number of collisions experienced while trying to send packets out the interface.
- **Queue** - The number of packets currently queued for transmission on the interface.
- **Stat** - Either "UP" or "DOWN" indicating whether the interface is active.

The values which are displayed when "Display Data" is set to "Active Configuration" are:

- **Name** - The name of the network interface. The Ethernet interface is named "ether0" and each interface through the serial ports is named "ptp", followed by a uniquely assigned number.
- **inet/dest** - For the Ethernet interface, the internet address of the PortMaster. For the ptp interfaces, the internet address of the remote system.
- **netmask** - The netmask of the inet/dest field.
- **Ipxnet** - The IPX network number of the interface.
- **Routing** - "Routing", "Sending", Listen", or "Quiet" indicating whether RIP protocol packets are being transmitted or received by the interface.

Administration Command Prompt Interface — CHAPTER 5

All administration activities of the PortMaster can be performed using an ASCII terminal connected to a PortMaster serial port or remotely using the telnet protocol to establish an administrative session on the PortMaster. When using an ASCII terminal, set the communication parameters of the terminal to match those which have been previously set for that port or to the default parameters if no settings have been made (Default: 9,600 baud, 8 data bits, 1 stop bit, and no parity). If the port settings are unknown, lifting diagnostic switch #1 (left-most in the bank of 5) will return port S0 to the default configuration.

Using the Commands

To use the ASCII Command Interface, you must login to the PortMaster using a special administrator's user name and password. This login can be initiated from any serial port configured either as a login or dialnet port, or through a telnet session to the TCP port number specified in the Global Telnet Access Port (default 23). At the login prompt enter:

```
login: !root
```

The PortMaster will prompt for a password. This is the PortMaster administration password. When shipped from the factory, there is no password. Upon entering the correct password, the PortMaster will display the prompt:

```
Command>
```

At this point you can begin to use the PortMaster commands. Each command responds to the minimum number of characters (at least two) that are unique to that command. Command entry is not case sensitive.

The User Commands

The following commands are available:

- **SET** - Set the serial port, ethernet port, and global parameters. Set values an parameters in tables.
- **SHOW** - Show the status of each port, all ports and global data, or entries in tables.
- **REBOOT** - Reboot the PortMaster to the current saved configuration.
- **RESET** - Reset a port (or ports) to the current stored configuration.
- **VERSION** - Display the version number of the PortMaster software.
- **QUIT, DONE, EXIT** - Leave the Command mode.
- **SAVE** - Save the current configuration to the PortMaster permanent configuration.
- **HELP** - Provide information on each of the PortMaster commands, including usage and syntax.
- **ADD** - Add entries to one of the local PortMaster tables.
- **DELETE** - Delete entries from one of the local PortMaster tables.
- **DIAL** - Begin dialing to one of the Dialnet Locations.
- **IFCONFIG** - Similar to the ifconfig command on UNIX systems, this provides configuration values for all active interfaces. It also allows modification of active values.
- **TELNET** - Allows you to telnet from the Command prompt to another host on the network.
- **TRACEROUTE** - Allows you to trace network routes when attempting to debug a problem.
- **PING** - Allows you to send and receive ICMP packets from the Command prompt.

● **PMLOGIN** - Allows you to establish a login using the PortMaster login service to a node on your network.

● **PTRACE** - Allows you to watch network traffic using a filter (see "Filters" later in this chapter).

● **RLOGIN** - Allows you to establish a login using the UNIX rlogin service to a node on your network.

Global Parameters

Global parameters are used to set system wide values and to enable supporting network services like DNS or Telnet access. For many applications the default settings for these parameters will be sufficient. If the PortMaster will be placed on an IPX network the "sysname" must be set.

The syntax for setting global parameters is:

SET *parameter value [options]*

Valid parameters and their associated values and options are:

SYSNAME - Set the global system name. The value is the name used for SNMP queries and IPX.

PASSWORD - The PortMaster administration password. The value is a string of up to 16 characters to be used for the administration password.

GATEWAY - The default gateway (router) internet address. The gateway address should be set using the standard "dot" notation (i.e., XXX.XXX.XXX.XXX where XXX is a decimal number between 0 and 255. An optional metric for the default route between 1 and 15 may be entered after the gateway address. The default value is 1.

IPXGATEWAY - The default IPX gateway (router) address. This should be entered in the format "Network_Number:Node_Address" (i.e., 00001234:00AABBCCDDEE). A metric value between 1 and 15 may be entered after the gateway address. The default value is 1.

DEBUG - The debugging mask for the PortMaster. Most values are reserved for use by Livingston Technical Support and are of little use to the administrator. The debug value of 0x51 allows the administrator to observe PPP configuration requests and acknowledgments. The output is sent to the defined system console. The console is set by using the command "set console". Setting debug to 0x0 disables the output.

NAMESVC - The service (NIS or DNS) used for resolving host names.

NAMESERVER - The name server IP address.

DOMAIN - The domain name to use on the name server. The value is the domain name.

DEFAULT - Default routing options for all interfaces. Valid values are:

On - The PortMaster will send default route information as part of its normal RIP messages and will accept default route information coming from other routers.

Broadcast - The PortMaster will send default route information as part of its normal RIP messages.

Listen - The PortMaster will accept default route information coming from other routers.

Off - The PortMaster will not send default route information to other routers and it will ignore all default route messages it receives.

SNMP - For managing SNMP. Valid values are:

On - To enable SNMP.

Off - To Disable SNMP.

Readcommunity - Sets the SNMP read community on the PortMaster.

Writecommunity - Sets the SNMP write community on the PortMaster.

HOST - The default host IP address for terminal server sessions. An optional value may be inserted before the IP address to specify alternate hosts. This extra value is a number between 1 and 4. "1" is the primary or default host and "2" through "4" are the alternate hosts.

ASSIGNED - The first assigned IP address for Dialnet Users. This address is used only for network login users who are using the PPP or SL/IP protocols, and are being assigned a temporary address for their active session.

TELNET - The telnet access port for the PortMaster. This value allows the administrator to use the telnet protocol to maintain the PortMaster. The value can be any number from 0 to 65536. If "0" is used, telnet administration will be disabled. The value "23" is the default TCP port number for telnet.

LOGHOST - The PortMaster supports "syslog" network accounting. The value is the IP address of the host the PortMaster will log to using facility "auth" and priority of "info" (auth.info). An example of a typical /etc /syslog.conf(5) entry follows:

auth.info /var/log/termlog

The syslogd(8) daemon doesn't create files, so before the logging can start the file must be created manually using touch(1). Finally, in order to cause syslogd to re-read the new entry in /etc/syslogd.conf, get the process ID of syslogd using ps and send it a hangup signal:

```
root@myhost# ps aux|grep syslogd
root   80  0.0  0.2   60   60 ?  S   Jan 24  0:50 syslogd
root@myhost# kill -HUP 80
```

Consult your system's *syslogd* and */etc/syslog.conf* manual pages for more information on this service.

AUTHENTIC - Set the primary RADIUS authentication server.

ALTERNATE - Set the alternate RADIUS authentication server.

SECRET - Set the RADIUS encryption secret. Refer to Chapter 6, "RADIUS" for more information on setting up RADIUS for use with the PortMaster.

Ethernet Parameters

Ethernet parameters are used to manage the PortMaster ethernet port. This port is identified as "ether0" and all commands should use this port name in the set command. Ethernet parameters include IP addresses, IPX network addresses and various settings for the ethernet interface.

The syntax for setting ethernet parameters is:

SET *ether0 parameter value [options]*

Any values which require an IP address should use the format:

XXX.XXX.XXX.XXX

where the XXX is a decimal number between 0 and 255.

Valid parameters and their associated values and options are:

ADDRESS - The value is the PortMaster ethernet IP address.

NETMASK - The subnetting IP address mask for the Ethernet interface.

BROADCAST - The broadcast address for the Ethernet interface. Valid values are "high", to use a host port of all ones; and "low" to use a host port of all zeros. The actual broadcast address is constructed from the IP address of the PortMaster and the netmask. The current standard is "high" but some networking products still use low. All hosts on a subnet should use the same broadcast value.

IPXNET - The IPX network number for the ethernet interface. This number should be entered in HEX format.

IPXFRAME - The Frame Type used when sending IPX packets out the Ethernet interface. Options include one of the following:

Ethernet_802.3

Ethernet_802.2

Ethernet_II

Ethernet_802.2_II

Consult with your Novell System Administrator for the IPX frame type in use on your network.

ROUTING - The routing options for the Ethernet interface. Valid values are:

On - The PortMaster will send RIP information to other computers attached to the local Ethernet and will accept RIP information from other routers on the local Ethernet.

Broadcast - The PortMaster will send RIP information to other computers attached to the local Ethernet.

Listen - The PortMaster will accept RIP information from other routers on the local Ethernet.

Off - The PortMaster will not send RIP information to the local Ethernet and it will ignore all RIP messages it receives on the local Ethernet.

IFILTER - Set the Input Filter for the Ethernet interface. When set, all packets received from the Ethernet interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Input Filters" toward the end of this chapter.

OFILTER - Set the Output Filter for the Ethernet Interface. When set, all packets sent to the Ethernet interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Output Filters" toward the end of this chapter.

IP - Whether or not to enable IP traffic on the Ethernet interface of the PortMaster. Valid values are "**enabled**" to enable IP traffic and "**disabled**" to disable IP traffic.

IPX - Whether or not to enable IPX traffic on the Ethernet interface of the PortMaster. Valid values are "**enabled**" to enable IPX traffic and "**disabled**" to disable IPX traffic.

Port Configurations

The following section describes the serial port parameters and each of the possible configuration parameters. Serial port parameters describe the type of service which will be available on that port as well as the specific data-communications parameters which are appropriate for communicating with the device attached to the port.

Setting the Serial Port Type

The syntax for setting the port type is:

SET *port_no type [device] [* NETWORK *dialnet_type]*

Where *port_no* is one of S0 through S29 and *type* is one of:

LOGIN - The specified port will display a login prompt to the user. After successful baud rate matching and receiving a login name, the user will be transferred directly to a login session on the host computer.

DEVICE - The port will operate as a host controlled device on the workstation. The Host Device field described below must be entered.

TWOWAY - The port operates in User Login mode if carrier is detected on pin 8 of the RS-232 connector (DCD). Otherwise it can be accessed as a host device on the computer. The Host Device field described below must be entered.

DISABLED - can be used for port P0 to disable the /dev entry. When reset, the P0 port will go to an idle (unused) state.

device is of the form:

/dev/*<tty_device>*

This is required in either the **Host Device** or **TwoWay** mode. The Host Device name is the name of a pseudo tty device in the /dev

directory. Standard device entries are:

/dev/ttyp0 - /dev/ttypf
/dev/ttyq0 - /dev/ttyqf
/dev/ttyr0 - /dev/ttyrf

See Appendix A for further information.

/dev/network may be used for specifying the port as a device when a physical port is not required or if one is not available.

NETWORK - If set to a type of NETWORK, one of four Dialnet values must be provided as an argument:

Hardwired - If the port is being used for a dedicated network connection between two sites. No modem dialing or authentication is required. The port immediately begins running the specified protocol. In this mode, none of the other port types can be used with Dialnet.

Dial In - In this mode, the port will accept dial-in only network connections. The remote system is required to enter a user name and password. Dial In network connections are controlled by the Users Table described later in this chapter.

Dial Out - In this mode, the port becomes available for dialing to remote destinations and initiating network connections to those destinations. Dial Out network connections are controlled by the Location Table described later in this chapter.

Two Way - In this mode, the port will accept dial-in network connections, as well as being available for dial out to remote destinations. In any of the three Dial modes, the port can also be configured to support other port operations concurrently. If one of the other port types is selected, that port type and **Dialnet** will be highlighted. If one of the other port types is selected, those port type parameters become available. For example:

```
set s7 twoway /dev/network network twoway
```

Allows the port to be used for regular user dial in and dial out, as well as permitting in and outbound network connections.

Setting Port Parameters

The syntax for setting port parameters is:

SET *port parameter value [parameter value ...]*

Where *port* is one of: S0 - S29

Parameter and *value* is one of:

SPEED - The baud rate for the port.

An extra value is entered after the "**SPEED**" key word to indicate which of the three optional baud rates is being set. Valid options are: **1**, **2**, or **3**. This is followed by the actual baud rate. Valid values are: **115200**; **57600**; **38400**; **19200**; **9600**; **4800**; **2400**; **1200**; **600**; **300**.

PARITY - The parity checking to be used for the port.

Valid values are: **EVEN**, **ODD**, or **NONE**

DATABITS - The number of databits per byte.

Valid values are: **8**, **7**, **6**, or **5**.

STOPBITS - The number of stop bits in the data frame.

Valid values are: **1** or **2**.

MODEM - Whether to observe the presence of the carrier detect signal.

Valid values are: **ON** or **OFF**.

XON/XOFF - Whether to use Xon/Xoff flow control.

This is a software flow control which is supported by most devices.

Valid values are: **ON** or **OFF**.

RTS/CTS - Whether to use RTS/CTS flow control.

This is for devices where hardware flow control is required. When the PortMaster is able to receive data from the attached device, it raises Request to Send (RTS) on pin 4 of the RS-232 connector. Output from the PortMaster will only occur if the Clear to Send (CTS) modem line on pin 5 of the RS-232 connector is raised by the attached device.

Valid values are: **ON** or **OFF**.

HOST - The host for this specific port.

This option determines which host the port connects to during an active session. Valid values are:

Default - In this mode the port uses the "default host" setting. See "Global Parameters" earlier in this chapter.

Prompt - In this mode, the user is given a host prompt before the standard login prompt. The user then is required to enter a valid host name or internet address for a host on the network. Entering PPP or SL/IP at the prompt will return a login prompt.

Hostname or **Internet Address** - The port is assigned to a specific host during an active session. An optional value may be inserted before the internet address to specify alternate hosts. This extra value is a number between 1 and 4. "1" is the primary host and "2" through "4" are the alternate hosts. Alternate host connections are only attempted if the primary host is unavailable (i.e., the host is down or network is unreachable). Alternate host entries are optional.

SERVICE_LOGIN - The port can be configured to use one of four different network services for establishing login sessions.

Valid values are:

PortMaster - This is the default service and can be used with any host workstation which has had a "Host Installation" performed from either **pminstall** or the install window of **pmconsole**. This is the preferred service because it makes the port operate like the serial ports physically installed in the workstation. In addition it is the most efficient and highest performance service available.

Rlogin - This service is supported by a large number of UNIX based computers. **Rlogin** should be used where it is impractical to use the PortMaster service.

Telnet - This service is supported by most TCP/IP implementations. Telnet should be selected in a network where mixed hardware and operating systems will be used by this port. The default TCP port number for telnet is 23, however an alternate port number may be entered following the **Telnet** parameter.

Netdata - This service can be used to create a virtual connection between a port and another serial port on a different PortMaster, or to a clear channel TCP connection on a Unix host. The default TCP port number for netdata is 6000, however an alternate port number may be entered following the **Netdata** parameter. The port on the remote PortMaster must be configured as a Host Device Port using the same service and TCP port number.

SERVICE_DEVICE - The port can be configured to use one of four different network device services. Valid values are:

PortMaster - This is the default service and can be used with any host which has had a "Host Installation" performed from either **pminstall** or the install window of **pmconsole**. This is the preferred service because it makes the port operate like the serial ports physically installed in the host. When selected, the port is accessed through a /dev/tty device on the host.

Rlogin - This service is supported by many UNIX based computers, and can be used to allow UNIX based hosts on the network to initiate an rlogin session to the PortMaster. Once the session is successfully established the host application will be able to directly read and write data to the serial port. If multiple ports on the PortMaster are configured to use this service it will create a pool of ports which can be accessed by other hosts. When all ports in the pool are in use new users will be given a "Connection Refused" message.

Telnet - This service is supported by most TCP/IP implementations. Once the session is successfully established, the host application will be able to directly read and write data to the serial port. If multiple ports on the PortMaster are configured to use this service it will create a pool of ports which can be accessed by other hosts. When all

ports are in use new users will be given a "Connection Refused" message. The default TCP port number for telnet is 23, however an alternate port number may be entered following the **Telnet** parameter.

Netdata - This service can be used for customized application programs that need a TCP connection directly to a serial port on the PortMaster. Programs which use the "socket" interface (or a similar TCP interface) are provided with a direct data link to the PortMaster serial port. Port operating parameters are pre-set by the administrator. The application can then open the socket connection and immediately begin reading and writing data to the PortMaster. No special option negotiation or protocol is required. The default TCP port number for netdata is 6000, however an alternate port number may be entered following the **Netdata** parameter. If multiple ports on the PortMaster are configured to use this service with the same TCP port number it will create a pool of ports which can be accessed by other hosts.

TERMTYPE - Sets the terminal type in the user's environment. This optional field is used in either **Login** or **TwoWay** mode. When a new session is established on the host workstation this terminal type will automatically be set in the user's environment. A valid entry from the termcap database should be entered. If this field in not entered the host workstation will assume a "dumb" terminal.

PROMPT - Customized user login prompt. This field allows the administrator to customize the login prompt the user will see. Any valid ASCII characters may be entered. The default is to display the Host Name followed by the word "login:". If the string "$hostname" is included in the login prompt, the active hostname is substituted for the string. An example for setting all the ports to display the same login message would be:

```
Command> set all prompt "foobar login:"
New Login Prompt:
"foobar login:"
For ports: S0 S1 S2 S3 S4 S5 S6 S7 S8 S9
```

OVERRIDE - Sets which configuration parameters can be overridden by the host. The PortMaster allows overrides to be set for Baud Rate, Parity, Databits, and Flow Control. This feature allows the host to alter the active parameters via software control (i.e., system ioctl calls). The default is that the Host can only turn Xon/Xoff flow control on and off. Two values are specified after the **OVERRIDE** parameter. The first one is the item to set. Valid values are: **XON/XOFF**, **BAUD**, **DATABITS**, or **PARITY**. The second value is either **On** or **Off**. "**On**" means the host can override the value. "**Off**" means the PortMaster configuration value is used and host attempts to change these values are ignored.

EXTENDED - Sets extended mode on or off. Valid values are: **On** or **Off**. When Extended mode is **On** more detailed output will be displayed in the **SHOW** command. For example, with extended mode set to **Off** the following information would be displayed:

```
Command> show s0
----------------- Current Status - Port S0 ----------------
          Status: USERNAME
           Input: 43                      Parity Errors:  0
          Output: 477                     Framing Errors: 0
         Pending: 0                       Overrun Errors: 0
                  Active Configuration    Default Configuration
                  --------------------    ---------------------
       Port Type: Login                   Login  (Security)
     Baud Rates: 9600                     9600,9600,9600
         Parity: none                     none
  Modem Control: off                      off
Terminal Type:
```

With extended mode set to On, the following information is displayed:

```
Command> show s0
---------------- Current Status - Port S0 -----------------
        Status: HOSTNAME
         Input: 43                          Parity Errors:  0
        Output: 485                        Framing Errors:  0
       Pending: 0                          Overrun Errors:  0

Active Configuration    Default Configuration  (* = Host
--------------------    ---------------------  Can Override)
     Port Type: Login                          Login  (Security)
 Login Service: PortMaster                     PortMaster
    Baud Rates: 9600                           9600,9600,9600
      Databits: 8                              8
      Stopbits: 1                              1
        Parity: none                           none
  Flow Control: Xon/Xoff                       Xon/Xoff*
 Modem Control: off                            off
         Hosts:                                prompt
 Terminal Type:
  Login Prompt: "foobar login:"
  Autolog Name:
```

USERNAME or **AUTOLOG** - Sets the Autolog name. If this field is entered, the user will not receive the standard login prompt. Instead, the PortMaster will automatically initiate a session on the Host Computer as if the user had typed the Autolog Name in response to the login prompt.

SECURITY - Sets the security level for this port. Valid values are **On** which disables **Pass Thru** logins and **Off** which enables **Pass Thru** logins. If **Pass Thru** logins are enabled (security set to **Off**) any user name which does not match the local **Users Table** will automatically be forwarded to the designated host for login and authentication. When using RADIUS security must be set to **On** in order for RADIUS daemon to perform lookups in the users file. See Chapter 6 "RADIUS" for more information on this service.

CONSOLE - Sets this port to the PortMaster system console.

MESSAGE - The login message to be displayed to the user prior to the login prompt. The value for this parameter is a string of up to 240 characters. New-lines are designated by using the carat symbol (^).

IDLETIME - The idle timeout specifies how long the PortMaster should wait after the activity on the port stops before disconnecting the session. The idle timeout is specified in minutes and can be any value from 0 to 240. If set to 0 no timeout will be used.

GROUP - This field is used by Dialnet for creating dial-out pools when establishing remote network connections.

ACCESS - This sets the access override for asynch ports and is used in conjunction with the **Access Filter**. Valid values are **On**"or **Off**. The default is "**Off**". When set to "**On**", users in the **Users Table** will be allowed to override the port's Access Filter with their own Access Filter by providing the correct username and password.

IFILTER (ACCESS FILTER) - This is the filter applied to a port configured to prompt the user for a host. For example, if a port has been configured for a host prompt and has an input filter allowing access only to a specified host, only requests from that prompt to the specified host will be allowed. The filter would be constructed as follows:

```
add filter host_access
set filter host_access 1 permit 192.9.200.99/32 192.9.200.1/32
save filter
set s1 ifilter host_access
reset s1
```

In the above example, anyone dialing in to the PortMaster with the address of 192.9.200.99 would only be allowed to access the host 192.9.200.1.

HANGUP - This controls whether the DTR signal on the RS-232 connector will be momentarily dropped to cause a hangup after the termination of a user session. If set to **Off**, DTR will not drop after the session terminates. If set to **On**, DTR will drop. The default is **On**.

Examples

Examples of the **SET** command are:

set s1 speed 2 115200

Sets the second baud rate to use for speed matching to 115200 baud.

set s1 login

Sets the Device Type on serial port S1 to User Login.

set s1 twoway /dev/ttyr0

Sets serial port S1 to a two-way device using /dev/ttyr0 as the device name on the host workstation.

set s1 message Welcome to the PortMaster^This is Port S1

Will display the login message:

```
Welcome to the PortMaster
This is Port S1
```

More than one argument/value can be set on the command line and commands may be abbreviated to their least uniqueness:

```
Command> add netu foo pass foo comp on addr 1.1.1.1 netm 255.255.255.0
New User successfully added
Command> sh user foo
   Username: foo                    Type: Dial-in Network User
    Address: 1.1.1.1              Netmask: 255.255.255.0
   Protocol: SLIP                 Options: Quiet, Listen, Compression
        MTU: 1006
```

In the above example, a **Network User** named *foo* is added with the **Password** of *foo*. **Compression** is turned **On** and the user's destination **Address** and **Netmask** are set. The other displayed values are the defaults for a **Network User**.

The **SET** command stores values in the dynamic RAM. No changes take effect until you enter **RESET** or an active session terminates. Since changes to these values are *only* kept in dynamic RAM **SAVE** must be entered in order to write them to nonvolatile FLASH. If **SAVE** is not entered, the entries will no longer exist after the PortMaster is rebooted.

Setting Dialnet Hardwired Port Parameters

Dialnet Hardwired ports are used for SLIP or PPP connections established between PortMasters or between a PortMaster and a host where no dialing sequence is required. For example, an installation using a synch to asynch converter where the connection is established over a dedicated telephone line, a Dialnet Hardwired Port would be used.

The syntax for setting port parameters is:

SET *port parameter value*

Where *port* is one of S0-S29.

Parameters are:

DESTINATION - The IP address of the remote PortMaster or computer using SL/IP or PPP. If destination is set to 255.255.255.255 for PPP connections the PortMaster will attempt to negotiate the remote IP address. If set to 0.0.0.0 for PPP connections, the port will be disabled.

NETMASK - The IP subnet mask for the destination address.

The above two parameters are entered in one of two ways:

```
set port_no destination 192.9.200.1 netm 255.255.255.0
- or -
set port_no destination 192.9.200.1
set port_no netmask 255.255.255.0
```

IPXNET - The IPX network number for the point to point connection. This number should be entered in HEX format. For example:

```
set ipxnet C009C801
```

Sets the IPX network number to the hex value for 192.9.200.1 which can be useful when using IPX in a mixed environment.

ROUTING - This indicates whether the PortMaster should use the RIP protocol through the Interface. The following options are available:

On - The PortMaster will send RIP information to a remote router or node and will accept RIP information from the remote router or node.

Broadcast - The PortMaster will send RIP information to the remote router or node, but will not accept RIP information from the remote router or node.

Listen - The PortMaster will not send RIP information to the remote router or node, but will accept RIP information from the remote router or node.

Off - The PortMaster will not send RIP information to the remote router, and will not accept RIP information from the remote router.

COMPRESS - Whether to enable Van Jacobson TCP/IP header compression. Valid values are: **On** or **Off**. When using PPP, this value is negotiated between the PortMaster and the remote node. With SL/IP it is *mandatory* that each end either specify compression as **On** or **Off**. If one end has compression **On** and the other has compression **Off**, the SL/IP connection will come up, but packets which can be compressed will not traverse the link.

PROTOCOL - The protocol to use for encapsulating packets. Valid values are:

SLIP - Use the Serial Line Internet Protocol.

PPP - Use the Point to Point Protocol.

MAP - The PPP Async map. This value should be entered in hex notation (i.e., 0x00000000). The PPP protocol supports the escaping of non-printing ASCII characters in the datastream. Escaping means that specified characters will not be sent through the line, but instead will be replaced by a special set of characters which the remote site will interpret as the original character. The PPP Async Map is a bit-map of characters which should be escaped. The first (or zero) bit corresponds to the first ASCII character "NULL" and so on. Most environments should be set to zero to achieve maximum throughput.

IFILTER - This sets the Input Filter for the interface. When specified, all packets received from the interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Input Filters" toward the end of this chapter.

OFILTER - This sets the Output Filter for the interface. When specified, all packets sent to the interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will leave the PortMaster. See "Output Filters" toward the end of this chapter.

MTU - This is the desired Maximum Transmission Unit to be used for the interface. PPP connections can be set to values from 100-1500 and the remote computer can negotiate a smaller value than the setting entered. SLIP connections can be set to values from 100-1006. Maximum Transmission Unit defines the largest "frame" or "packet" which can be sent through this connection. If a packet is too large to fit, it will be automatically fragmented into smaller pieces by the PortMaster. Setting this to smaller (i.e., less than 300) values can be useful when using multi-line load balancing or for enhanced interactive performance while running concurrent file transfers.

SHOW Command

The **SHOW** command allows you to look at the current settings for any of the serial ports and the ethernet interface. It also lets you look at available memory, current network connections, network statistics, current routes, and the PortMaster tables.

The syntax for the show command is:

SHOW keyword

- or -

SHOW TABLE tablename

Valid keywords are:

- **Ether0** - This keyword will display ethernet settings.
- **S0 - S29** - Show all settings for a communications port.
- **All** - Show summary of all communications ports.
- **Sessions** - All active sessions on the PortMaster.
- **Routes** - Show the routing table. Fields displayed are:

  destination - the remote host or network

  gateway - the next hop system

  metric - the hop count to the destination

  interface - which network interface to use

  flags - locally defined:

```
"H" - A host route
"N" - A network or subnet route
"S" - A static route
"L" - A route to a directly attached network or host
"D" - A dynamic route
"C" - A route which has recently changed
"O" - An obsolete route (scheduled for deletion)
```

- **Netstats** - Input/output statistics summary for all network interfaces.
- **User** - The configuration settings for a user in the user table.

- **Location** - The configuration settings for a dialnet location.
- **Table** - Show summary of the specified table. Valid values are:

  Location - This is the table where outbound PPP or SLIP dial scripts are stored. Only the location names are displayed. For configuration information use the command **SHOW** *Location_Name*.

  User - This is the table where login information is kept for users configured locally on the PortMaster. Passwords themselves are not displayed, nor are specific configurations displayed. To see the specific configuration of a user use the command **SHOW USER** *User_Name*.

  Filter - The list of packet and access control filters stored in the PortMaster. Only the filter names are displayed. For detailed filter information use the command **SHOW FILTER** *Filter_Name or* **SHOW SAPFILTER** *SAP_Filter_Name*

  Host - The hosts table stored locally on the PortMaster

- **Global** - This keyword will display system wide configuration values. These values include:

  System Name - The name of the PortMaster (also known as the SNMP system name).

  Default Host - The primary host for establishing terminal server connections.

  Alternate Hosts - A list of up to 3 hosts for terminal server access for use when the primary host is unavailable.

  IP Gateway - The default IP gateway (or route) for the PortMaster.

  Default Route - Whether the PortMaster is advertising or listening for default routes from other routers.

  Name Service - One of either NIS or DNS.

  Name Server - The IP address of the host providing Name Service.

  Domain - The name of the NIS or DNS domain.

  Telnet Access Port - The TCP port number of the telnet administration service.

  Loghost - The IP address of the host running the syslogd facility.

  Assigned Address - The first address in the assigned pool.

RADIUS Server - The IP address of the server running the RADIUS authentication service.

Alternate Server - The alternate RADIUS server.

- **Arp** *Interface_name* - Show arp table for indicated interface.
- **Memory** - Show system memory usage.
- **Netconns** - Show all PortMaster TCP, UDP, and SPX network connections.

For example:

show all

Shows the settings of global parameters and a summary of each of the individual ports. The display is similar to the **View** window in **pmconsole** described in chapters 3 and 4.

show s1

Displays the full set of configuration values for serial port S1. If **Extended** mode is turned on, a more detailed set of information will be displayed.

show table hosts

Displays the currently stored hosts table.

IFCONFIG Command

When the **IFCONFIG** command is entered, the active configuration of each network interface is displayed. Each interface is displayed in two lines. The first line has the name of the interface (i.e., ether0, ptp1) and various flags for that interface. Possible flags are:

IP_UP - The interface is UP and running the IP protocol.

IP_DOWN - The interface is DOWN and IP is not in use.

IPX_UP - The interface is UP and running the IPX protocol.

IPX_DOWN - The interface is DOWN and IPX is not in use.

BROADCAST - The network is a broadcast network (i.e., ethernet).

LISTEN - RIP packets are being received on this interface.

RIPSEND - RIP packets are being received and sent to and from the interface.

POINT_TO_POINT - The network is a point to point connection.

PRIVATE - No routing information will be transmitted on this interface. If "private" is not shown as a flag, routing information will be transmitted to the interface.

SUSPENDED - This On-Demand Dialnet interface is available for use, but does not have an active telephone connection to the remote site.

The second and third line will show:

inet - the internet address of the interface.

dest - the destination internet address if it is a point to point connection.

netmask - The netmask for the "inet" or "dest".

broadcast - The broadcast address if it is an ethernet interface.

mtu - The maximum transmission unit for the interface.

ipxnet - The IPX network number for the interface.

ipxframe - The IPX frame type for the interface.

IFCONFIG may also be used to change interface characteristics in real-time in much the same way as the UNIX command. For example:

ifconfig ether0 netmask 255.255.255.0

would change the netmask to 255.255.255.0 on the ethernet interface. Since this change takes place immediately, care must be taken to avoid disrupting the network or active sessions on the PortMaster.

PING Command

The ping command allows the administrator to verify that the PortMaster can communicate with another node on the network. This is accomplished by sending an ICMP echo request to the remote node and listening for the corresponding echo reply from that node. The ping command takes a host name or IP Address as its argument as long as the hostname can be resolved by the PortMaster.

PMLOGIN Command

Pmlogin initiates a login session to a node on the network using the PortMaster network connection service. This command is only available from an administrative session on a serial port.

PTRACE Command

The **ptrace** command allows the administrator to monitor specific network traffic received by the PortMaster. The **ptrace** command takes the name of a packet filter as its argument. When enabled, packets received by the PortMaster are evaluated against the packet filter. If the packet is "permitted" through the filter, a user-readable message indicating the source and destination, protocol, and other protocol specific information are displayed to the administrator. By using a defined packet filter, the administrator can narrow the output down to the specific traffic they are interested in monitoring. By specifying the **ptrace** command with no filter, packet tracing is disabled.

When accessing the PortMaster via a telnet session, care should be taken to filter out the administrative telnet packets. Otherwise, **ptrace** will report packets from the administrators own ptrace output, causing a large

amount of unusable packet tracing information. Following is an example filter for **ptrace**:

```
1 deny 0.0.0.0/0 0.0.0.0/0 tcp src eq 23
2 deny 0.0.0.0/0 0.0.0.0/0 tcp dst eq 23
3 permit 0.0.0.0/0 0.0.0.0/0
```

To set up this filter, enter the following:

```
set filter foo 1 deny 0.0.0.0/0 0.0.0.0/0 tcp src eq 23
set filter foo 2 deny 0.0.0.0/0 0.0.0.0/0 tcp dst eq 23
set filter foo 3 permit
```

Then type:

```
ptrace foo
```

To stop the output from ptrace, simply enter *ptrace*

This example filters out all telnet packets while allowing all ip traffic to be seen for the purpose of debugging. This filter is only required when debugging from a telnet session. When debugging from a terminal session (connected directly to one of the serial ports) a filter is not required.

REBOOT Command

Reboots the PortMaster, reloading the currently saved parameters. All ports will be set to the state of the last saved configuration. The syntax is:

REBOOT

RESET Command

Reset a port to its currently stored values. Any terminal that is logged in through the PortMaster will be disconnected and all active sessions will be terminated. The syntax is:

RESET *port*
- or -
RESET *all*

Where *port* is one of S0 - S29 and *all* represents all serial ports currently installed on the PortMaster.

RLOGIN Command

Rlogin initiates a login session to a host on the network using the rlogin network connection service. This command is only available from an administrative session on a serial port.

TELNET Command

Telnet initiates a login session to a host on the network using the telnet network connection service. This command takes a host name or IP address as its argument. Telnet will accept a TCP port number as an argument for establishing a connection (the default is port 23).

TRACEROUTE Command

The traceroute command allows the administrator to identify all of the routers (and the path) to a remote host. This is accomplished by sending special UDP packets to the host and listening for ICMP messages from the routers. The traceroute command takes a host name or IP Address as its argument and returns a list of routers in the order seen.

QUIT, DONE, EXIT Command

These commands will log you out of the PortMaster command mode and return you to login mode.

SAVE Command

Saves the current configurations in the PortMaster non-volatile storage. The syntax is:

SAVE *port*

- or -

SAVE *all*

Where *port* is one of S0 - S29. Using **SAVE** *all* will store all global parameters, port parameters, and tables in the PortMaster. The **SAVE** command can also be used to save routes, users, locations, hosts, SNMP and Filters.

HELP Command

Provides information on the usage and syntax of the PortMaster commands. For example:

```
Command> help set
                              SET OPTIONS
General Parameters
----------------------------------------  ------------------------------------
s0-s29,p0 - Set configuration for a port   telnet     - Set the TCP access port
ether0    - Set configuration of ethernet  password   - Set the admin password
default   - Set the use of default routes  loghost    - Set the syslog host
domain    - Set the NIS or DNS domain      host       - Set default login host
nameserver- Set the NIS or DNS server      assigned   - Set pooled IP address
namesvc   - Set NIS or DNS service         sysname    - Set SNMP system name
gateway   - Set the default route          console    - Attach to sys console
ipxgateway- Set the IPX default route
Authentication Parameters                  Entries in Tables
----------------------------------------  ------------------------------------
authentic - Set the primary auth server    location - Set value for a location
alternate - Set the alternate auth server  user     - Set value for a user
secret    - Set the encryption secret      snmp     - Set value for SNMP
                                           filter   - Set rule for IP filter
                                           sapfilter- Set rule for SAP filter
                                           ipxfilter- Set rule for IPX filter

Use "help set option" for further assistance
```

```
Command> help set user
Network User Parameters                    Login User Parameters
----------------------------------------  ------------------------------------
address  - Set User's Internet address     dialback - Set the telephone number
compression - Set header VJ compression    host - Set the login host
dialback - Set the dialback location       password - Set the user's password
map - PPP async map in HEX format          service - Set the login service
mtu - Desired Maximum transmission unit    ifilter - Set access filter
netmask  - Set the Netmask
password - Set the user's password
protocol - Set the Protocol (SLIP, PPP)
routing  - Type of routing
ifilter  - Set input packet filter
ofilter  - Set output packet filter

Usage: set user User_Name option value
```

```
Command> help set s0
Data Communications Parameters          General Parameters
--------------------------------------  --------------------------------------
databits - Set the number of databits   console - Set the system console
modem - Set hardware carrier detect     extended - Set extended port features
override - Set host overrides           network - Set SLIP or PPP use
parity - Set the parity                 twoway - Set both login & device use
rts/cts - Set RTS/CTS flow control      access - Set access override
speed - Set the port speed
stopbits - Set the number of stopbits   Outbound Parameters
xon/xoff - Set Xon/Xoff flow control    --------------------------------------
hangup - Set line hangup with DTR       device - Enable outbound device use
                                        group - Set the Dialnet group number
Login Parameters                        service_dev - Set the device service
--------------------------------------
login - Enable user logins              Hardwired Dialnet Connection Parameters
host - Set the login host for the port  --------------------------------------
message - Set the welcome message       compress - Set VJ header compression
prompt - Set the login prompt           destination - Set remote IP address
security - Set pass-thru login access   ifilter/ofilter - Set packet filters
service_login - Set the login service   map - Set the PPP async map
termtype - Set the terminal type        mtu - Set maximum transmission unit
username - Set the Autolog username     protocol - Set the network protocol
idletime - Set the idle timeout         routing - Set type of routing
Use "help set s0 parameter" for further assistance

Command> help set s0 speed
Usage: set Port_Name speed [1-3] baudrate

Command> help set s0 device
Usage: set Port_Name [login] [device tty_device]
                     [network hardwire|dialin|dialout|twoway]
```

Managing the Hosts Table

Each device which uses TCP/IP is assigned a unique internet address. Internet addresses are four byte numerical values. To make it easier to remember these values, most systems on the network support a way of aliasing the internet address to some unique name. This is done on UNIX systems in the /etc/hosts file. The PortMaster also supports the same capability by maintaining a local hosts table.

The PortMaster hosts table should be used when any of the ports are set to prompt the user for a host name on the network. This table is then consulted to determine the correct internet address of the host.

If the hostname specified by the user is not found in the hosts table, then the PortMaster will attempt to match the hostname using the Network Information Service (NIS), also known as "YP", or DNS, the Domain Name Service. See the section "Setting Global Parameters" for more information on choosing and setting the name service appropriate to your network.

Four commands have been established for managing the local hosts table:

- **ADD** - adds entries to the local hosts table.
- **DELETE** - deletes entries from the local hosts table.
- **SHOW** - shows the entries in the local hosts table.
- **SAVE** - saves the entries to non-volatile storage.

ADD Command

Add an entry to the local hosts table. The syntax is:

ADD host *internet_address hostname*

internet_address - is a valid host internet address in the form:

XXX.XXX.XXX.XXX

where XXX is a decimal number between 0 and 255.

hostname - is a character string of printable characters.

DELETE Command

Delete an entry from the local hosts table. The syntax is:

DELETE host *internet_address*

- OR -

DELETE host *hostname*

internet_address - is a valid host internet address in the form:

XXX.XXX.XXX.XXX

where XXX is a decimal number between 0 and 255.

hostname - is a character string of printable characters.

SHOW Command

List a summary of the Hosts Table or show the specific configuration values for a single user.

The syntax for the show command is:

SHOW hosts

SAVE Command

Stores the Hosts Table in the PortMaster's non-volatile storage.The syntax for the save command is:

SAVE hosts

Managing the Users Table

The Users Table provides login security for users to establish login sessions or for incoming Dialnet network connections or user login sessions.

Serial ports configured to accept login sessions initially prompt for a user login name. After receiving the login name, the PortMaster checks the name against the list of names in the local Users Table. If found, the PortMaster initiates password authentication of the user. If successfully validated (the password received matches the password stored in the Users Table) the PortMaster begins the session defined for the user. If RADIUS has been implemented the internal Users Table is still consulted first. Not finding an entry for the user internally the authentication request is passed to RADIUS instead of the UNIX host. For more information about RADIUS see Chapter 6, "RADIUS".

Four types of users can be created: **Network User/Normal**, **Network User/Dialback**, **Login User/Normal** and **Login User/Dialback**.

Network User/Normal users are allowed to immediately establish an active PPP or SLIP connection to the network. **Network User/Dialback** users are disconnected by the PortMaster which then dials back to the user's remote modem using a predefined telephone number. **Login User/Normal** users are allowed to immediately begin an active session on a host on the network. **Login User/Dialback** users are disconnected by the PortMaster which then automatically dials back to the user's remote modem using a predefined telephone number. This feature allows for enhanced security or to simplify telephone charge-back.

If the login name does not match an entry in the **Users Table** and the port is configured to support **Pass Thru** login it forwards the session to the designated host on the local network for password authentication. If your site is using the RADIUS authentication server the validation and login attributes are performed by the server, if they are not found in the **Users Table** the request is passed on to RADIUS for authentication. Note that **Pass Thru** login must be disabled for RADIUS to receive and process the authentication request.

Five commands can be used for managing the local users table:

- **ADD** - adds new users.
- **DELETE** - deletes existing users.
- **SHOW** - shows settings for users.
- **SET** - sets parameters for existing users.
- **SAVE** - saves changes to the users table to nonvolatile storage.

ADD Command

Add an entry to the local users table. The syntax for login users (i.e., not PPP or SLIP) is:

ADD User *user_name* **Password** *user_password*

user_name - is a 1-8 character name for the new user.
user_password - is a 0-16 character password for the new user.

Add an entry for network users. The syntax is:

ADD Netuser *netuser_name* **Password** *netuser_password*

netuser_name - is a 1-8 character name for the new Netuser.
netuser_password - is a 0-16 character password for the new Netuser.

DELETE Command

Delete a user from the passwords table. The syntax is:

DELETE User *user_name*

user_name is a 1-8 character name of an existing user.

SHOW Command

List a summary of the Users Table or show the specific configuration values for a single user.

The syntax for the show command is:

SHOW Table Users
- or -
SHOW User *user_name*

SET Command

The set command can be used to configure specific values for Login Users. The syntax of the command is:

SET User *user_name parameter value [parameter value ...]*

Where *user_name* is the name of an existing **Login User**. Several parameters may be set in each command in a single command statement. Valid parameters are:

Password

The password for the user. The value is a string of up to 16 ASCII characters. The syntax of the command is:

SET User *user_name* **Password** *User_Password*

Setting Login User Parameters

Dialback

The dialback telephone number for the user. This is the string of characters which would follow the Hayes compatible "ATDT" command. If a telephone number is entered, the user will be automatically changed to a dialback user. If the word "none" is entered as the dialback value, the user will be changed into a normal Login User. The syntax of the command is:

SET User *user_name* **Dialback** *555-1212*

Host

This field defines which network host the user's session will be forwarded to. The three values and their meanings are:

Default - Connect the user to the defined host for this serial port. Consult the serial port setting for the defined host.

Prompt - Allow the user to select a host (either by IP address or name) to begin a login session.

IP Address - Connect the user to the host specifically entered. A valid hostname or IP address should be entered here. The syntax for the command is one of:

SET User *user_name* **Host** *default*

SET User *user_name* **Host** *prompt*

SET User *user_name* **Host** *ip_address*

Service

The user can be set to use any of the available PortMaster Login Services. For a complete description of these services, consult the login service descriptions defined in the extended serial port parameters section of this manual. Valid values are: PortMaster, Rlogin, Telnet, or Netdata. The TCP port number may also be specified after the name of the service. The syntax for the command is:

SET User *user_name service [option]*

Ifilter

An access control filter can be set for a user if they are set to be prompted for a host. The Ifilter can be any valid filter name from the Packet Filter Table. See "Packet Filters" later in this chapter for more information.

Setting Network User Parameters

The syntax for setting network user parameters is:

SET User *user_name parameter value*

Where **USER** is the login name of the PortMaster User. If the user will be using either SLIP or PPP the SET command argument is:

SET Netuser *user_name parameter value*

parameter and *value* are one of:

Address (or Destination)

Set (or assign) the user's IP address. Valid values are:

Assigned - The PortMaster will assign a temporary IP address for this session. This address will be retrieved from the pool of addresses being maintained by the PortMaster. See the Global Configuration section for more information on Assigned Addresses.

Negotiated - This option is valid only for PPP sessions. The PortMaster will attempt to learn the IP address of the remote node automatically.

IP Address - A specific address in standard "dot" notation. Setting the address to 0.0.0.0 will disable the IP protocol for this user.

IPXnet - The IPX Network Address for the point to point connection should be entered. This value must be in HEX format.

Compression

Set VJ header compression for a PPP or SL/IP user. Valid values are either **On** or **Off**. This indicates whether the PortMaster should use Van Jacobson TCP/IP header compression. This option can increase the performance of interactive TCP sessions if both sides of the link support this option. When configuring SLIP connections, both sides must be configured identically. When configuring PPP connections, if compression is enabled and the remote side doesn't support compression, the PortMaster will dynamically disable this feature.

Dialback

Set (or assign) the user's dialback location. This is the name of the location stored in the PortMaster Location Table. After authenticating a Dialback Network User, the PortMaster will disconnect the active connection and dial to the specified location.

Map

Set the PPP async map in hexadecimal format. The PPP protocol supports the escaping of non-printing ASCII in the data stream. Escaping means that specified characters will not be sent through the line, but instead will be replaced by a special set of characters which the remote site will interpret as the original character. The PPP Async Map is a bit-map of characters which should be escaped. The first (or zero) bit corresponds to the first ASCII character "NULL" and so on. Most environments should be set to zero to achieve maximum throughput.

MTU

This is the desired Maximum Transmission Unit to be used for the Interface. PPP connections can be set to values from 100-1500 octets and the remote computer can negotiate a smaller value than the setting entered. SLIP connections can be set to values from 100-1006. Maximum Transmission Unit defines the largest "frame" or "packet" which can be sent through this connection. If a packet is too large to fit, it will be automatically fragmented into smaller pieces by the PortMaster. Setting this to smaller (i.e., less than 300) values can be useful when using multi-line load balancing or for enhanced interactive performance while running concurrent file transfers.

Netmask

The value is the netmask of the system at the remote end of the dial-up connection should be entered in standard "dot" notation.

Protocol

Set (or assign) a network user's encapsulation protocol. Valid values are SL/IP or PPP.

Routing

Set a PPP or SL/IP user's routing method. Valid options are one of:

On - The PortMaster will send RIP information to the remote device and will accept RIP information from the remote device.

Broadcast - The PortMaster will broadcast RIP information to the remote device.

Listen - The PortMaster will listen for RIP information from the remote device.

Off - The PortMaster will not send RIP information to the remote device and it will ignore all RIP messages it receives from the remote device.

Ifilter

Set (or assign) the user's Input Packet Filter. When specified, all packets received from the serial interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to enter the PortMaster. See "Packet Filters" toward the end of this chapter.

Ofilter

Set (or assign) the user's Output Packet Filter. When specified, packets being sent to the serial interface will be evaluated against the rule set for this filter. Only packets which are permitted by this filter will be allowed to leave the PortMaster. See "Packet Filters" later in this chapter.

SAVE Command

Stores the Users Table in the PortMaster's non-volatile storage.The syntax for the save command is:

SAVE Users

PPP Auto-Detect and PAP/CHAP negotiation

The PortMaster supports Auto-Detect PPP for use with the PAP and CHAP methods of login authentication. If the device at the remote end of the connection supports PAP or CHAP, when the login or host prompt is provided by the PortMaster it will automatically detect PPP frames and the authentication will begin.

The CHAP challenge process (a practical example)

At the Corporate site is a PortMaster with the SNMP sysname of **pm1**. When the remote PortMaster **pmremote** establishes a connection and begins sending PPP frames, **pm1** becomes responsible for issuing a CHAP challenge. Inside that challenge is an ID string containing the name **pm1**. An entry for **pm1** is *required* in the PortMaster Users Table on **pmremote**.

When **pmremote** receives the challenge it makes a lookup in its local **Users Table**. Finding the entry, it passes the password through the MD5 encryption algorithm and forms a response back to **pm1**. Contained within the response is an ID string containing the SNMP sysname of **pmremote**. **pm1** then looks in its Users Table for an entry for **pmremote** and uses that password to validate the CHAP response received from **pmremote**.

If the password comparison is successful, **pm1** will send a "CHAP successful" message back to **pmremote** and the connection is complete. If the MD5 comparison fails, a "CHAP failure" message is sent to **pmremote** and the process repeats.

If the **pm1** wishes to use RADIUS to authenticate the remote PortMaster, the ID string and the password can be stored in the RADIUS users file on the RADIUS server. The password must be in clear text for the MD5 comparison to succeed.

Each PortMaster involved in this authentication must have an entry in its User Table which contains the SNMP sysname of the other PortMaster.

Note: The passwords must be identical.

To clarify, the password for **pm1** is known as a *shared secret*, it is the same password used by **pmremote**. The name of the remote PortMaster and an identical password *must* be in the PortMaster Users Table on **pm1** or in the RADIUS users table on the RADIUS server for **pm1.**

For more information on the PortMaster authentication decision making tree, refer to Chapter 6, RADIUS.

Managing the Location Table

The Location Table is used for all dial out network connections to remote locations. Each entry specifies a remote location, the operational parameters for that location, and information on how to establish a connection to that location.

Five commands are available for managing locations:

- **ADD** Command - adds entries to the local Locations table.
- **DELETE** Command - deletes entries from the local Locations table.
- **SET** Command - sets or modifies location configuration parameters.
- **SHOW** Command - shows a summary of the locations table or details a specific location.
- **SAVE** Command - saves locations into permanent configuration.

ADD Command

Add an entry to the local Locations table. The syntax is:

ADD location *location_name*

Where:

location_name - The name of the remote location. This can be any 12 character name to identify the remote location. It is generally not the name of a single system, but rather an identifier which represents the entire location, e.g., the city or the company name at that location.

DELETE Command

Delete an entry from the local Locations table. The syntax is:

DELETE location *location_name*

Where:

location_name - is the name of a previously created location.

SET Command

Once a location has been created, all of the configuration parameters associated with that location can be set or modified with the SET command. The syntax is:

SET *location_name parameter value*

Where:

location_name - is the name of a previously created location.

parameter is one of:

ON_DEMAND - This parameter notifies the PortMaster to dial and establish a connection to the remote location only when packets are queued for that location. In this mode the PortMaster creates a network interface and the appropriate routing information to notify the attached local area network of the connectivity to the remote site. This is done even though there may not be an actual physical connection to that site at the time. There is no value required for this setting.

Note: When switching a location from Manual to On_demand make sure the dial-out connection has been closed (i.e., Reset the serial port) before updating the location table.

CONTINUOUS - This parameter notifies the PortMaster to always keep the dial-up connection to the remote site active. If the telephone line is lost, the PortMaster will re-dial to that location. The re-dial mechanism in continuous mode is based on a back-off algorithm which begins at 30 seconds and continues until six attempts have been made at which point it logs the failure to syslogd and quits until manual intervention is made by the administrator.

MANUAL - This parameter notifies the PortMaster to only dial to the remote location when an operator requests the connection. This can be done with the **Dial** command or it can be invoked from the **pmdial** program installed on one of the UNIX systems on the network. This also allows connections to be scheduled by using the UNIX cron scheduler to call **pmdial**.

DESTINATION - The internet address of the system at the remote end of the dial-up connection. For SL/IP connections, the IP address or a valid host name of the system at the remote end of the dial-up connection should be entered.

For PPP connections, the destination can be negotiated. In this mode, the PortMaster can automatically learn the IP address of the remote system. Enter "255.255.255.255" as the destination to enable this feature. This can only be used for **Manual** or **Continuous** connections. **On_Demand** locations must use a specified address.

NETMASK - The netmask of the system at the remote end of the dial-up connection. A valid netmask using standard dot notation should be entered as the value.

IPXNET - This is the IPX network number assigned to the point to point connection. This value must be in HEX format.

ROUTING - This indicates whether the PortMaster should use the RIP protocol through the Interface. The following options are available:

On - The PortMaster will send RIP information to the remote computer and will accept RIP information from the remote computer.

Broadcast - The PortMaster will send RIP information to the remote computer, but will not accept RIP information from the remote computer.

Listen - The PortMaster will not send RIP information to the remote computer, but will accept RIP information from the remote computer.

Off - The PortMaster will not send RIP information to the remote computer, and will not accept RIP information from the remote computer.

COMPRESS - Whether to enable Van Jacobson TCP/IP header compression. Valid values are: ON or OFF. This indicates whether the PortMaster should use Van Jacobson TCP/IP header compression. This option can increase the performance of interactive TCP sessions if both sides of the link support this option. When configuring SLIP connections, both sides must be configured identically. For PPP, if compression is enabled and the remote side

does not support compression the PortMaster will dynamically disable this feature.

PROTOCOL - The protocol to use for encapsulating packets. Valid values are:

SLIP - Use the Serial Line Internet Protocol.

PPP - Use the Point to Point Protocol.

MAP - The PPP Async map. This value should be entered in hex notation (i.e., 0x00000000). The PPP protocol supports the escaping of non-printing ASCII in the data stream. Escaping means that specified characters will not be sent through the line, but instead will be replaced by a special set of characters which the remote site will interpret as the original character. The PPP Async Map is a bit-map of characters which should be escaped. The first (or zero) bit corresponds to the first ASCII character "NULL" and so on. Most environments should be set to zero to achieve maximum throughput.

MTU - This is the desired Maximum Transmission Unit to be used for the Interface. PPP connections can be set to values from 100-1500 and the remote computer can negotiate a smaller value than the setting entered. SLIP connections can be set to values from 100-1006. Maximum Transmission Unit defines the largest "frame" or "packet" which can be sent through this connection. If a packet is too large to fit, it will be automatically fragmented into smaller pieces by the PortMaster. Setting this to smaller (i.e., less than 300) values can be useful when using multi-line load balancing or for enhanced interactive performance while running concurrent file transfers.

IDLETIME - For Manual and On-Demand type locations this specifies the number of minutes the line should be idle (no network traffic to the remote site) before disconnecting the telephone connection. A value between 0 and 240 can be specified. If 0 is chosen, the connection will not time out.

MAXPORTS - The number of dial-out ports the PortMaster can use for this network connection. If 0 is selected dialing to this location will be disabled. If more than 1 is selected the PortMaster will use the "High Water Mark" to decide when to open and dial additional lines.

If more than one line is open to the remote location the PortMaster will automatically use load balancing to achieve the maximum throughput of all lines combined. If multiple lines are open the "Idle Timeout" value will be used to decide when to disconnect unneeded lines. A value between 0 and 99 may be entered.

HIGH_WATER - The number of bytes of queued network traffic required to open an additional dial-out line to the remote site. This value is only used when "Maximum Ports" is greater than 1 and there are available modems on the PortMaster. Setting a very small number will cause the PortMaster to quickly use all of the ports. Generally, interactive terminal traffic has no more than a few hundred bytes queued at any one time. However, file transfers (i.e., ftp) will queue several thousand bytes. These size differences should be used when deciding what number to use for the High Water Mark. A value between 0 and 65535 may be entered.

GROUP - The modem pool group to which this location is assigned. Only modem ports which are configured with this Group Number will be available for dial-out to this location. This can be used to reserve modems for dial-up to specific locations or to differentiate different types of modems which would be compatible with the remote location. A value between 0 and 99 may be entered.

SCRIPT - The dial command script is used to issue commands to the modem (or other similar equipment) to dial the correct number and establish the link. In addition, this script is used for authentication (password security) at the remote site. The syntax is:

SET *location_name* **SCRIPT** *l_no send expect [l_no send expect]*

Where *l_no* is a number between 1 and 6. *send* is a string of up to 30 characters surrounded by double quotes. *expect* is a string of up to 30 characters surrounded by double quotes. Each *l_no* represents a send-expect pair, or combination.
Each "Send" string is issued out of the PortMaster serial port to the modem or remote computer. Each "Expect" string is used by the

PortMaster to verify that the previous "Send" string was properly received by the modem or remote computer and the PortMaster should transmit the next "Send" string.

For example if the remote system is prompting for a login id, it may issued the string:

```
Please enter your login:
```

The Expect string in the Dial Command Script could simple look for "ogin:".

Any printing ASCII character can be placed in the send or reply strings. In addition, the following special characters are available:

\r - This is replaced by the ASCII carriage return.

\n - This is replaced by the ASCII line feed.

\0XX - This is replaced by the octal digit in the XX.
\\ - This is replaced by the single backslash (\).

Generally Send strings would end with the "\r" character.

It is recommended that the last entry in the Dial Command Script be an Expect string which indicates that the remote location is ready to begin receiving network packets. This is used to activate the data link protocol coming from the PortMaster. When connecting to a remote PortMaster the final reply string to look for should be "SL/IP" for SLIP connections and "PPP" for PPP connections. For other products, consult that vendors users manual.

The following Dial Command Script is an example of how to establish a connection between two PortMasters which have modems supporting the "AT" dial command syntax:

```
Send                    Expect
--------------------    ----------------
ATDT18005551212\r       CONNECT
\r                      login:
my_login_name\r         ssword:
my_password\r           SL/IP
```

The "18005551212" would be replaced by the actual telephone number of the remote modem. "my_login_name" is replaced by the user name for your location. "my_password" is replaced by the password set up at the remote site which corresponds to the user name. The command syntax for creating this entry would be:

```
set location example script 1 "atdt18005551212\r" "CONNECT"
set location example script 2 "\r" "ogin:"
set location example script 3 "my_login_name\r" "ssword:"
set location example script 4 "my_password\r" "SL/IP"
```

SHOW Command

List a summary of the **Location Table** or the detail of a specific location.

The syntax for the show command is:

SHOW TABLE LOCATION - to display a summary of the location table.

SHOW *location_name* - where *location_name* is the name of a previously created location. This will display all of the configuration information for the location.

SAVE Command

Save Locations into the permanent PortMaster configuration. The syntax is:

SAVE LOCATION

Managing the Routes Table

The PortMaster Routes table is used when static network routes are required. Static routes are required when the user chooses not to run the Routing Information Protocol (RIP) on the PortMaster, or when hosts or networks attached to the PortMaster do not have the ability to run the RIP protocol. The static routing table contains three entries:

Destination - This is the host or network to which the PortMaster will be required to send packets.

Gateway - This is the directly connected host through which packets should be forwarded to reach the above destination.

Metric - This is a metric representing the cost of sending the packet through the above gateway. Generally metric is the HOP count to the remote network. This would be the number of gateways through which the packet must traverse to reach its destination.

Four commands are available for managing static routes:

- **ADD** Command - adds static route.
- **DELETE** Command - deletes existing static route.
- **SHOW** Command - shows values in the static routes table.
- **SAVE** Command - saves changes to the static routes table.

ADD Command

Add an entry to the static routes table. The syntax is:

ADD Route *destination gateway metric*

destination - is the destination IP address.
gateway - is the gateway IP address.
metric - is the hop count to the remote destination.

DELETE Command

Delete a static route. The syntax is:

DELETE Route *destination gateway*

destination - is the destination IP address.

SHOW Command

Shows the Routes Table in the PortMaster's non-volatile storage.

The syntax for the save command is:

SHOW Table routes

SAVE Command

Stores the Routes Table in the PortMaster's non-volatile storage.

The syntax for the save command is:

SAVE routes

PPP CHAP authentication

The PortMaster supports CHAP method of login authentication. If there is a PortMaster at the remote end of the connection, it will immediately begin the PPP negotiation once the connections is established. The PortMaster supports login authentication through CHAP protocol from the remote device; when it receives the challenge, it uses the id string (the remote system name) contained in that challenge to locate an entry in the local User Table. It will then use the user it finds to construct the correct authentication response to the challenge. Refer to the detailed discussion on PAP and CHAP authentication earlier in this chapter.

Dialing Out to Remote Locations

On-demand or Continuous dial-out locations automatically initiate dialing to a remote location. Manual connections require a system administrator or a scheduler to initiate dial-out connections. The command prompt interface provides a facility for the system administrator to initiate the dial-out operation and if necessary to monitor the progress of the dial-out operation.

When setting up a new On-demand location it is recommended to first set up the location as a manual dial-out site for testing purposes and then later switch the location type to On-demand.

Note: When switching a location from Manual to On-demand, make sure the dial-out connection has been closed (reset the serial port) before updating the location table.

To initiate dial-out connections via a scheduler (i.e., cron in UNIX systems) or from a UNIX command line prompt see the **pmdial** command in the UNIX Utilities section of this manual.

To dial to a remote location from the Command Prompt Interface, the **dial** command may be used. The syntax for this command is:

DIAL *location_name* [-x]

Where "*location_name*" is the name of the saved location in the **Location Table**. If no additional parameters are specified the PortMaster will provide notification of which port is being used for dialing and will return to the "Command>" prompt. If the "-x" option is specified, the PortMaster will display the actual dialing progress. The "send" message shows the exact string of characters being sent out the serial port to the modem or remote system enclosed in parentheses. The "expect" message shows the response string the PortMaster is expecting as a reply enclosed in parentheses. Immediately following the "expect" string are the characters actually being received by the PortMaster from the modem or remote system. When the PortMaster successfully receives the string is is searching for, it will display ":got it" followed by the next send message.

If the dial script completes successfully, the message "Connection Succeeded" will be displayed. Otherwise, after timing out the message "Connection Failed" will be displayed To hangup the connection reset the port in use with the **reset** command.

Packet Filters

Packet filters are used primarily as a security mechanism in networks which cross organizational or corporate boundaries. They are useful in limiting certain kinds of inter-network communications by specifically permitting or denying the passage of packets through network interfaces. By designing appropriate filters, administrators can control access to specific computers, networks, and network services.

Packet filters require the analysis of the header information contained in each packet sent or received through a network interface. This header information is evaluated against a set of rules which allows the packet to pass freely through the interface (and on to its destination in the network) or causes the packet to be discarded without forwarding.

The packet filtering mechanism is designed around two primary objectives. First, maximum flexibility is required to allow the administrator to achieve the desired results without compromising security. Second, efficiency is desirable to maximize network performance. Specific features which support these objectives are:

- **Input** and **Output Filters** - Each interface can be assigned both an input packet filter as well as an output packet filter. This is especially useful in routers with more than two network interfaces and it simplifies the design task. The administrator can evaluate each interface, where its destination is, and the mix of traffic both inbound and outbound desired for the interface. This capability also has the potential to decrease the number of rules contained in the filter because fewer network numbers need to be included.

- **Source and Destination Address Filtering** - Both source and destination addresses are evaluated in the rule list. Also, the number of significant bits to use in IP address comparisons can be set. This allows filtering based on specific hosts, subnets, or network numbers.

- **Protocol Filtering** - Specific protocols can be handled separately in the packet filters. These include TCP, UDP, and ICMP for IP and IPX.

- **Source and Destination Port Filtering** - The source and destination port numbers can be used in the rule set to control availability of specific

network services. This includes evaluation based upon whether the port number is less than, equal to, or greater than a specific value.

- **Established Session Filtering** - The status of TCP connections can be used as part of the rule set. This allows users in a network to open connections to external networks without allowing external users access to the local network.

- **Unlimited Number of Rules** - Each filter can have a large number of rules specified. This is only limited by available memory within the router.

- **Simple Rule Creation** - The command syntax for creating specific rules allows the administrator to specify only as much information as is necessary to specify the rule. For example if the rule is not based upon specific source and destination IP address, these addresses can be omitted from the specification of the rule.

- **Ordered Rule Processing** - Rules are processed in the order in which they are specified in the rule set. This eliminates ambiguity about how a specific packet would be handled, and allows more flexibility in creating a packet filter.

Filter Organization

The PortMaster maintains a table of packet filters in its permanent configuration memory. These filters can be created or modified at any time and are independent of any active packet filters. Each filter is assigned a name of up to 15 characters in length. Each packet filter has three sets of rules. These are IP rules, IPX rules and SAP rules. Each rule set is made up of a list of rules which are numbered starting at 1. A packet filter when initially created contains no rules.

IP and IPX packet filters are attached to interfaces as either input or output filters. SAP filters are attached only as output filters. For serial interfaces, the packet filter is enabled when it transitions to the UP state (i.e., after a reset on the port). The Ethernet interface filter is enabled as soon as the name of the input or output filter is specified.

Packet filters are attached to interfaces as either input filters or output filters. For serial interfaces, the packet filter is enabled at the time it

transitions to the UP state (i.e., after a reset on the physical port). The Ethernet interface filter is enabled as soon as the name of the input or output filter is specified.

Filter Creation

New packet filters are created with the "add filter" command. It is recommended that a specific naming convention be used to differentiate the uses of various filters. For example, the following names could be used:

internet.in - The input filter to be used for the link to the Internet.
internet.out - The output filter to be used for the link to the Internet.
s1.in - The input filter for serial port S1.
ether.out - The output filter for the ethernet interface.
project1.out - The output filter to be used during a special project.

The syntax of the "**add filter**" command is:

add filter Filter_Name

Filter_Name is the name to be assigned to a filter.

Setting Filter Rules

Once a filter has been created, the "**set filter**", "**set ipxfilter**", or "**set sapfilter**" commands are used to add, modify or delete specific rules.

IP Rules

The syntax for specifying an IP rule is:

set Filter *filter_name* **Rule_no** *action*

[*Source_address/bits Destination_address/bits*]

[*Protocol* [*src lt\|eq\|gt Value*] [*dst lt\|eq\|gt Value*]

[*established*]

Filter_Name - is the name of an existing filter.

Rule_no - is a number up to the highest previously set Rule_no plus 1

(i.e., if there are 4 existing rules, Rule_no can be from 1 to 5). If an existing rule number is specified, it is replaced by the new rule. If no parameters are specified for the rule, that rule is deleted.

Valid actions are:

permit - Permit the packet to pass freely through the interface.

deny - Stop the packet from traveling through the interface.

Source_address/bits - specify the comparison with the source IP Address contained in the packet. The number of bits (0-32) are first extracted from the IP Address in the packet (i.e., if 24 bits is specified, a packet with the source address of 192.9.200.1 would become 192.9.200.0 since 24 bits are used to represent the first 3 bytes of the address). The most common bit counts would be:

0 - To match packets with any source IP Address.
16 - To look at only the network number of a class B IP Address.
24 - To look at only the network number of a class C IP Address.
32 - To look at the entire IP Address.

The resulting value is then compared with the specific source address.

Destination_address/bits - specify the comparison with the destination IP Address contained in the packet. The number of bits (0-32) are first extracted from the IP Address in the packet. The resulting value is then compared with the specific destination address.

Protocol - The protocol of the packet may be specified. Valid values are TCP, UDP or ICMP.

Options - Each protocol supports a specific list of options:

TCP - This type of rule supports filtering on source and destination port numbers as well as the established state of the connection. The syntax for TCP options is:

[src eqlgtllt port_number] [dst eqlgtllt port_number] [estab]

Where:

src - indicates a comparison should be made with the source TCP port

number.

dst - indicates a comparison should be made with the destination TCP port number.

eq - indicates that the port number in the packet should be tested to see if it is equal to the port number specified in the rule.

gt - indicates the the port number in the packet should be tested to see if it is greater than the port number specified in the rule.

lt - indicates that the port number in the packet should be tested to see if it is less than the port number specified in the rule.

estab - indicates that the packet should be tested to see if it is for an established TCP network connection. If this key word is specified packets being sent to establish new TCP connections would not match this rule.

UDP - This type of rule supports filtering on source and destination port numbers. The syntax for UDP options is:

[src eq|gt|lt port_number] [dst eq|gt|lt port_number]

Where:

src - indicates a comparison should be made with the source UDP port number.

dst - indicates a comparison should be made with the destination UDP port number.

eq - indicates that the port number in the packet should be tested to see if it is equal to the port number specified in the rule.

gt - indicates the the port number in the packet should be tested to see if it is greater than the port number specified in the rule.

lt - indicates that the port number in the packet should be tested to see if it is less than the port number specified in the rule.

ICMP - This type of rule supports filtering on type of ICMP message. The syntax for ICMP options is:

[src eq icmp_message_type]

Where a comparison is made with the ICMP message type contained in the packet.

IPX Rules

The syntax for specifying an IPX rule is:

set ipxfilter Name Rule_no *action [keyword value] [keyword value]* ....

Name - is the name of an existing filter.

Rule_no - is a number up to the highest previously set Rule_no plus 1 (i.e., if there are 4 existing rules, Rule_no can be from 1 to 5). If an existing rule number is specified, it is replaced by the new rule. If no parameters are specified for the rule, that rule is deleted.

Valid actions are:

permit - Permit the packet to pass freely through the interface.

deny - Stop the packet from traveling through the interface.

Valid keywords are:

srcnet - Specifies the comparison with the source IPX Network Address contained in the packet. This value should be specified in HEX format.

dstnet - Specifies the comparison with the destination IPX Network Address contained in the packet. This value should be specified in HEX format.

srchost - Specifies the comparison with the source IPX Node Address contained in the packet. This value should be specified in HEX format.

dsthost - Specifies the comparison with the destination IPX Node Address contained in the packet. This value should be specified in HEX format.

srcsocket - Specifies the comparison with the source IPX socket number contained in the packet. A second keyword indicating the type of comparison must be specified. Valid comparison types are "equal", "lessthan" or "greaterthan". Following the comparison keyword, a

numeric value should be specified in HEX format.

dstsocket - Specifies the comparison with the destination IPX socket number contained in the packet. A second keyword indicating the type of comparison must be specified. Valid comparison types are "equal", "lessthan" or "greaterthan". Following the comparison keyword, a numeric value should be specified in HEX format

SAP Rules

The syntax for specifying a SAP rule is:

set sapfilter Name Rule_no *action [keyword value] [keyword value]* ....

Name - is the name of an existing filter.

Rule_no - is a number up to the highest previously set Rule_no plus 1 (i.e., if there are 4 existing rules, Rule_no can be from 1 to 5). If an existing rule number is specified, it is replaced by the new rule. If no parameters are specified for the rule, that rule is deleted.

Valid actions are:

permit - Permit the service to be advertised on this interface.

deny - Stop the service from being advertised on the interface.

Valid keywords are:

server - Specifies the comparison with the name of the server which is advertising its service.

network - Specifies the comparison with the server's IPX Network Address. This value should be specified in HEX format.

host - Specifies the comparison with the server's IPX Node Address. This value should be specified in HEX format.

socket - Specifies the comparison with the server's IPX socket number . A second keyword indicating the type of comparison must be specified. Valid comparison types are "equal", "lessthan" or "greaterthan". Following the comparison keyword, a numeric value should be specified in HEX format.

Deleting Filters

The "**delete filter**" command is used to remove a packet filter from the table. The syntax of the command is:

delete filter Filter_Name

Filter_Name - is the name of an existing filter.

Viewing Filters

The "**show**" command can be used to view the list of packet filters and the contents of each filter. To view the list of all packet filters use the command:

show table filter

To view the contents of a specific filter use the command:

show filter Filter_Name

Saving Filters

To save the table of packet filters use the command:

save filter

Filter names for specific interfaces are saved through the normal configuration save commands (i.e., "**save all**" or "**save s1**").

Packet Processing

When packets are received on an interface the active input filter for that interface is evaluated before forwarding the packet through the PortMaster.

Before packets are transmitted on an interface the active output filter for that interface is evaluated before transmitting.

Each rule is evaluated in the order the rules are specified. As soon as the packet matches one rule, that rule's action is immediately taken and no further processing is performed on the packet. If no rules match the

specific packet, the packet is "denied" and it is discarded. Whenever a packet is discarded, the PortMaster automatically generates and ICMP Host Unreachable message back to the originator.

It is recommended that packets which represent the highest volume of traffic through an interface be specified early in the list of rules. This will decrease the overhead of processing these packets and therefore increase overall performance.

Ethernet Interface Filters

The "set" command is used to establish specific input and output packet filters for the Ethernet interface. To set an input filter use the command:

set ether0 ifilter Filter_Name

Where **Filter_Name** is the name of an entry in the filter table. To set an output filter use the command:

set ether0 ofilter Filter_Name

If no name is specified, or if the named filter does not exist, packet filtering is disabled. Packet filtering is enabled or disabled on the ethernet interface immediately after executing the above **set** command.

Hardwired Serial Interface Filters

The "**set**" command is used to establish specific input and output packet filters for hardwired serial ports. To set an input filter use the command:

set Port_Name ifilter Filter_Name

Port_name - is the name of a port on the PortMaster (i.e., S1, S2...)

Filter_Name - is the name of an entry in the filter table.

To set an output filter use the command:

set Port_Name ofilter Filter_Name

If no name is specified, or the named filter does not exist, packet filtering is disabled. Packet filtering is enabled or disabled on serial interfaces when the port is reset, and the network connection is re-established.

Dial-In User Filters

For PortMasters using dial-up SLIP or PPP, input and output filters are assigned to the user instead of the serial port. When a user makes a PPP or SLIP connection the designated filters are assigned to the user's port. The "set user" command is used to assign filters to specific users.

To set an input filter for a user use the following command:

set user User_Name ifilter Filter_Name

User_Name - is the name of a user in the PortMaster **Users Table**

Filter_Name - is the name of an entry in the filter table.

To set an output filter for a user use the following command:

set user User_Name ofilter Filter_Name

User_Name - is the name of a user in the PortMaster **Users Table**

Filter_Name - is the name of an entry in the filter table.

Dial-Out Location Filters

For the PortMaster Communications Servers which support dial-out SLIP and PPP, input and output filters are assigned to the "location" rather than to the serial port. When a PPP or SLIP connection is established to a remote site the designated filters are attached to the port through which the connection is attached. The "set" command is used to assign filters to specific locations. To set an input filter for a location use the following command:

set Location_Name ifilter Filter_Name

Location_Name - is the name of a location in the PortMaster location table

Filter_Name - is the name of an entry in the filter table.

To set an output filter for a location use the following command:

set user Location_Name ofilter Filter_Name

Location_Name - is the name of a location in the PortMaster location table

Filter_Name - is the name of an entry in the filter table.

Examples

Because of the flexibility provided through the PortMaster packet filtering system, it is possible to specify filters which do not achieve the desired results. Great care should be taken to evaluate the types of traffic which a specific filter allows to pass through an interface. If possible, testing should be performed from both sides of the filtering interface to verify that the filter is operating correctly.

The following example could be used at a site which has an Internet connection and wishes to gain access to the Internet through a PortMaster serial port without exposing their site (and its network) to outside people and organizations. This filter would designate one system on the local network for all Electronic Mail communications with the Internet. It would also designate one system for all FTP access from the Internet. In addition, it will allow local users to Telnet and FTP to remote sites. Finally, it will allow DNS (Domain Name Service) to work between the Internet and the local site. For the purposes of this example, the local site will use network number 192.9.200.0, the E-mail server will be at address 192.9.200.1 and the FTP server will be at address 192.9.200.2.

```
#
#               Allow our users to open Telnet sessions with the Internet
#
set filter s1.in  1 permit tcp src eq 23 estab
set filter s1.out 1 permit tcp dst eq 23
#
#               Allow our users to open an FTP session with the Internet
#
set filter s1.in  2 permit tcp src eq 21 estab
set filter s1.out 2 permit tcp dst eq 21
set filter s1.in  3 permit tcp src eq 20 dst gt 1023
```

```
set filter s1.out 3 permit tcp dst eq 20
#
#               Allow DNS to pass through
#
set filter s1.in  4 permit udp dst eq 53
set filter s1.out 4 permit udp dst eq 53
#
#               Allow the Internet to open an SMTP session with our server
#
set filter s1.in  5 permit 0.0.0.0/0 192.9.200.1/32 tcp dst eq 25
set filter s1.out 5 permit 192.9.200.1/32 0.0.0.0/0 tcp src eq 25 estab
#
#               Allow our server to open an SMTP session with the Internet
#
set filter s1.in  6 permit 0.0.0.0/0 192.9.200.1/32 tcp src eq 25 estab
set filter s1.out 6 permit 192.9.200.1/32 0.0.0.0/0 tcp dst eq 25
#
#Allow the Internet to open an FTP and FTP-data session with our server
#
set filter s1.in  7 permit 0.0.0.0/0 192.9.200.2/32 tcp dst eq 21
set filter s1.out 7 permit 192.9.200.2/32 0.0.0.0/0 tcp src eq 21 estab
set filter s1.in  8 permit 0.0.0.0/0 192.9.200.2/32 tcp dst eq 20 estab
set filter s1.out 8 permit 192.9.200.2/32 0.0.0.0/0 tcp src eq 20
#
#               Allow ICMP for debugging
#
set filter s1.in  9 permit icmp
set filter s1.out 9 permit icmp
#
#               End of Example
```

save filter
set s1 ifilter s1.in
set s1 ofilter s1.out
save s1
reset s1

Configuring SNMP

The PortMaster provides support for using the Simple Network Management Protocol (SNMP) for getting and setting network management data. Specifically it provides the industry standard MIB-2 variables. These variables are described in the MIB distributed with the standard UNIX software. This MIB along with configuration files for various network management packages can be found in the "snmp" directory of the software.

Enabling SNMP

To enable or disable SNMP use for the PortMaster use to command:

SET SNMP on

- or -

SET SNMP off

Setting Community Names

The read and write communities to be used by the PortMaster can be set to any value. The SNMP community names are generally used to segregate administrative management communities. This should be set to match the read and write community settings of your SNMP management software. To set the SNMP read community use the command:

SET SNMP Readcommunity *Community_Name*

Community_Name is the name of the SNMP read community. To set the SNMP write community use the command:

SET SNMP Writecommunity *Community_Name*

Community_Name is the name of the SNMP write community.

Setting Read Hosts

For security purposes, the hosts which are allowed to perform SNMP gets can be set on the PortMaster. The syntax for this command is:

ADD snmphost reader *Host_Name*

Host_Name is one of the following:

Any - All hosts using the correct read community will be allowed to retrieve SNMP data from the PortMaster.

None - No SNMP reads will be responded to by the PortMaster.

IP Address - The IP address of the host to add to the list of valid SNMP readers.

Setting Write Hosts

For security purposes, the hosts which are allowed to perform SNMP gets can be set on the PortMaster. The syntax for this command is:

ADD snmphost writer *Host_Name*

Host_Name is one of the following:

Any - All hosts using the correct read community will be allowed to retrieve SNMP data from the PortMaster.

None - No SNMP reads will be responded to by the PortMaster.

IP Address - The IP address of the host to add to the list of valid SNMP readers.

Saving SNMP Configurations

After modifying SNMP configuration values, the SNMP table should be saved to non-volatile storage. This can be done by using the command:

SAVE snmp

Viewing SNMP Configurations

SNMP settings may be viewed by using the command:

SHOW Table snmp

RADIUS CHAPTER 6

Introduction

RADIUS (Remote Access Dialup User Service) is a protocol by which users (and in some cases systems) are provided access to secure networks through a centrally managed server. Authentication is provided for a variety of services (login, dialback, SLIP, PPP, etc.). When passwords are exchanged between the PortMaster and the RADIUS server they are encrypted using a shared secret as the encryption key.

Installation

To install RADIUS on a UNIX host, follow the guidelines below:

1) Run **pminstall**.

2) Select option 5, "RADIUS Installation".

3) Log on to your PortMaster(s) and define the Primary and Secondary Servers and set the encryption key (Secret). This procedure is described in Chapter 3 for X-Windows, Chapter 4 for an ASCII terminal, and in Chapter 5 for the Command Prompt Interface.

4) Set values in the clients and users file as described below.

Administration

The users file (located in /etc/raddb by default) uses "attribute/value pairs" provided in the dictionary file. The dictionary file can be modified, but it is not recommended unless you *thoroughly* understand the uses of RADIUS.

User Service Types

Under RADIUS, there are essentially five types of service users can be defined to make use of. They are:

- Login-User
- Framed-User
- Dialback-Login-User
- Dialback-Framed-User
- Outbound-User

Login-User

When defined, this field specifies the users will be allowed direct access to the host or network as defined, upon proper entry of their User Name and Password.

Framed-User

When defined, this field specifies whether the user is authorized to make either a SL/IP or PPP network connection. Optionally, the **Framed-Protocol, Framed-Address,** and **Framed-Netmask** fields must also be specified. Optionally, the **Framed-Routing** and **Framed-Compression** fields may also be defined These fields are described later in this section.

Dialback-Login-User

When defined, this field specifies the user is to be dialed back at a pre-defined telephone number following proper entry of their User Name and Password.

Dialback-Framed-User

When defined, this field specifies the user is allowed either a SL/IP or PPP connection and is to be dialed back at a pre-defined telephone number following proper entry of their User Name and Password. The Dialback telephone number and associated information is maintained in the Location Table.

Outbound-User

When defined, this user will be authenticated through RADIUS when

using the outbound modem pools. See Appendix E, Outbound Security for more information on its use.

Attribute/Value Pairs

This section contains dictionary translations for parsing RADIUS requests and generating responses. All transactions are composed of Attribute/Value Pairs. Values should be stored in the user file with dictionary value translations for ease of administration. The format for all entries except the userid is: attribute=<value>.

Login/Password Attributes

User-Name
This string attribute denotes the User (Login Name) to be authenticated.

Password
This string attribute has a value pair which can either be a quoted clear-text password maintained in the users file or a quoted value of UNIX which forces RADIUS to use /etc/passwd on the RADIUS host or (if NIS is being used) query the NIS server for password authentication.

Client-Id
This field, which must be entered in the standard dotted (".") internet notation, contains the IP address of the PortMaster which is used in the authentication of a user.

Client-Port-Id
This field identifies a PortMaster port which is used in the authentication of a user.

Framed Attributes

Framed-Protocol
This field is used to identify the user as either a SL/IP or PPP user. The default for a User Type of Network User is PPP.

Framed-Address
This field is used to specify the destination IP address or host name of the authenticated Network User. If the PortMaster is configured to use Assigned addresses the default action will be to assign an address to the Network User, otherwise the default action is to negotiate the address.

Framed-Netmask
This field is used to specify the destination netmask of the authenticated network user. The default netmask is 255.255.255.255

Framed-ipxnet
This field is used to specify the IPX network number of the authenticated Network User. This number should be specified in HEX format.

Framed-Routing
This field defines the RIP routing options, there are four possible values which can be specified here, the default is "None". The descriptions of these values follows:

None
If None is specified (or if the field is omitted), RIP (Routing Information Protocol) packets are disabled on the Dial In User's Interface.

Broadcast
If Broadcast is specified, RIP packets are allowed to be sent across the interface.

Listen
If Listen is specified, RIP packets are allowed to be received across the interface.

Broadcast-Listen
If Broadcast-Listen is specified, RIP packets are allowed in both directions across the interface.

Framed-Filter-Id
This field identifies the Packet Filter which has been set up on the PortMaster from which the user is accessing the network. If a user can

access multiple PortMasters on a network, each PortMaster must have identical filters installed. Note that when entering a name into this field that name is mapped in the format of ID.in or ID.out depending on whether an Input Filter or and Output Filter is being defined. If the Framed-Filter-Id is named, for example, FredFilter, internally the PortMaster uses a filter named FredFilter.out.

Framed-MTU
This field specifies the Maximum Transmission Unit allowed across the serial network connection. The maximum for SL/IP must be specified as 1006 while PPP can use an MTU of 1500. The default is 1500 bytes.

Framed-Compression
This field specifies whether or not to use Van-Jacobson header compression. The possible values are Van-Jacobson TCP-IP, or None. Since the default protocol is PPP, the default for compression is "**On**".

Login-Host
This field identifies the host to which a login user is connected.

Login-Service
This field has four possible settings. They are:

Telnet
Uses the "telnet" (port 23 by default) protocol to establish a connection with the host.
Rlogin
Uses the "rlogin" (port 513 by default) protocol to establish a connection with the host.

TCP-Clear
Uses the PortMaster "Netdata" (port 6000 by default) protocol to establish a connection with the host.

PortMaster

Uses the PortMaster "pmd" (port 1642) protocol to establish a connection with the host.

Login-TCP-Port
When defined, this field is used to force a user's connection to a specific TCP port number (such as 23, the default telnet port).

Dialback-No
This field must be defined in order to utilize the dialback facility of the PortMaster. It is a string which contains the telephone number to be dialed by the PortMaster after successful authentication.

Expiration
This numerical field specifies the amount of time before a password will expire. This is expressed as "December 12, 1999", for example.

Framed-Route
This field allows for the specification of a static route. There can be as many "Framed-Routes" as required for the remote connection. The format of this attribute is Framed-Route="destination gateway metric" where destination is the destination host or network, gateway is the node which provides the route to the host or network, and metric is the cost, or "hop-count" to the gateway. If the connection has been configured to use Assigned Addresses or if the address is negotiated, the notation of 0.0.0.0 will cause the gateway to be learned.

Users file examples

Following are some example of how a users file might be set up using a few of the facilities of the RADIUS server.

Login-User:

```
fred    Password = "UNIX"
        User-Service-Type = Login-User,
        Login-Host = powerhost,
        Login-Service = PortMaster
```

In the above example, the Login ID of "fred" has his password maintained either in /etc/passwd or through NIS. This user would literally login (at the login: prompt) as "fred". The default host is a host which can be looked up successfully through /etc/hosts or a name service such as NIS or DNS. RADIUS also supports C2 security.
Finally, fred's login service is defined as PortMaster. Notice that the username/password line does *not* have a comma following the entry, while the each line of options does. Further, note that the last line of the entry does *not* have a comma which indicates the end of the entry for the user. This is because the first line contains the "Authentication Items" and the remaining lines are known as the "Response Items".

Dialback-Login-User

```
bfred   Password = "somethingclever"
        User-Service-Type = Dialback-User,
        Dialback-No = "18005551212",
        Login-Host = powerhost,
        Login-Service = PortMaster
```

In the above example, notice the Password entry "somethingclever". This is literally the string the user fred enters at the password: prompt. Except for the "Dialback-User" and the "Dialback-No" entries, the user is treated no differently than the earlier example for fred.

Framed-User

```
sfred   Password = "UNIX", Client-Id=portmaster1, Client-Port-Id=1
        User-Service-Type = Framed-User,
        Framed-Protocol = SLIP,
        Framed-Address = 199.199.1.50,
        Framed-Netmask = 255.255.255.0,
        Framed-Routing = None,
        Framed-Compression = Van-Jacobsen-TCP-IP,
        Framed-MTU = 1006
```

In the above example, a SL/IP user with the login ID of sfred has his password maintained either in /etc/passwd or in NIS and has a defined protocol of SL/IP. The Client-ID and Client-Port-Id settings force fred to only be allowed to login on Port S0 of portmaster1. Further, the destination address has been set to 199.199.1.50 and the netmask has been defined as 255.255.255.0. The netmask must match that of the destination network. By setting the Framed-Routing to "None", no RIP packets will be sent or received across the interface; note that if the Framed-Routing entry were simply not included, no RIP packets would be sent or received across the interface. Also, having defined Framed-Compression, the Van Jacobsen header compression has been enabled. Finally, the Maximum Transmission Unit has been set to 1006 which is the highest allowed by the SL/IP protocol.

Dialback-Framed-User

```
sbfred  Password = "UNIX"
        User-Service-Type = Dialback-Framed-User,
        Dialback-Name = "f_location",
```

In this example, the user sfred is defined as a Dialback Framed User using SL/IP. The field "Dialback-Name" is used to specify the name of the Location Table entry to be used for dialing to the user's location.

Managing the clients file

The clients file is a file in the format of:

PortMaster_Name *Encryption_Key*

Where PortMaster_Name is the name of the PortMaster using RADIUS and Encryption_Key is the RADIUS "secret" being used by that PortMaster. This style of management allows the flexibility of each PortMaster having a separate "secret" or Encryption Key.
This is used in conjunction with the RADIUS client functions described in the sections appropriate to your environment - refer to Chapter 3 for management under X-Windows, Chapter 4 for management with an ASCII Terminal, and Chapter 5 for management from the Command Prompt Interface.

Using /dev Entries APPENDIX A

On UNIX systems there is a directory called /dev. This directory lists device names. Some devices are pseudo-devices, or pseudo-tty's. A pseudo-tty device is a virtual device that acts like a serial device. Most UNIX systems support at least 255. Each connection to the PortMaster requires a pseudo-tty device. Other software programs use pseudo-tty devices too. These include; X-Windows, rlogin, rsh, etc.

To use a pseudo-device, the operating system has to have support for the device. The second requirement to access a device, is an entry in /dev naming that device.

If the command:

ls -l /dev/ttyr0

is performed, the following entry would be displayed:

```
crw-rw-rw-  1 root      20,  32 Sep  2 08:20 /dev/ttyr0
```

This indicates that /dev/ttyr0 has major device number 20 (a pseudo tty) and minor device 32 (the 33'rd minor device number).

The implementation of pseudo-devices varies from system to system. Therefore, it is important to understand how your Unix operating system makes use of them. Consult the documentation which accompanies your Unix software release for further information in their use.

Using Default /dev Entries

To use the default /dev devices, simply use the path and name of the device, for example:

/dev/ttyr0

The port types Device and TwoWay require a device name, found in the /dev directory. Some UNIX releases allow the number of pseudo ttys configured into the kernel to be customized. Check your system documentation for instructions on adding pseudo tty devices.

Modifying your UNIX kernel

This section describes the steps required to modify the kernel of a system running SunOS 4.x. This can be used as a reference for other UNIX systems. Refer to your systems installation documentation for complete descriptions of these steps. For the Sun, the System and Network Administration Guide has a chapter "Reconfiguring the System Kernel". In the generic configuration file, in the /sys/<*arch*>/conf directory (where <*arch*> is the machine architecture - sun3, sun4, sun4c), there is a line dealing with pseudo-tty devices. This line sets the default number of pseudo-tty devices to 48:

```
pseudo-device  pty    #pseudo-tty's, also needed for SunView
```

Change the entry from 'pty' to 'pty64' and you will set the number of pseudo-tty devices to 64. Append any number you wish, up to 255 to the 'pty' entry. No number defaults to 48 devices. You will then need to rebuild your kernel, as described in the Sun documentation.

Using MAKEDEV

The last step is to make entries in /dev to match the operating system. The first 64 are created using a program called MAKEDEV. During a standard installation the first 48 device entries will be automatically created. They are:

/dev/ttyp0 - /dev/ttypf
/dev/ttyq0 - /dev/ttyqf
/dev/ttyr0 - /dev/ttyrf

An additional 16 may be created using MAKEDEV which is located in the /dev directory. Use the command:

MAKEDEV pty3

and /dev/ttys0 - /dev/ttysf will be created.

Note for System V Release 4 (Solaris 2.x):

Because of the implementation of pseudo-tty's under Solaris, care must be taken in choosing unique tty names. The pseudo-ttys selected under Solaris *must* begin with /dev/tty*, where * represents the actual tty name/number chosen for the Device Service.

Utilities APPENDIX B

pmcommand

The pmcommand utility allows the administrator to download an ASCII command file to the PortMaster. The syntax of this command is:

pmcommand [-nostop] PM_Name PM_Password Command_File

Where:

-nostop - tells pmcommand not to stop executing if there is an error in the command script. Without this option, any errors detected in commands will cause the script to immediately stop executing.

PM_Name - is the name or IP address of the PortMaster.

PM_Password - is the administration password for the PortMaster.

Command_File - is the name of the file containing PortMaster commands. All commands described in the "Command Prompt Interface" can be placed in this file.

pmdial

The pmdial utility allows manual or scheduled Dialnet connections to be initiated by the PortMaster from a host on the network. The syntax of this command is:

pmdial [-v] PM_Name PM_Password Location_Name

Where:

-v - tells pmdial to display the execution of the dial script as it proceeds on the PortMaster.

PM_Name - is the name or IP address of the PortMaster.

PM_Password - is the administration password for the PortMaster.

Location_Name - is the name of a Dialnet Location in the PortMaster Location Table.

For more information on Dialnet locations and dialing to those locations, consult the Dialnet User's Manual.

pmreset

The pmreset utility allows the system administrator to reset any or all ports on the PortMaster from a remote host. This can be embedded in a shell script or called directly by the administrator. The syntax of this command is:

pmreset PM_Name PM_Password Port_Name

Where:

PM_Name - is the name or IP address of the PortMaster.

PM_Password - is the administration password for the PortMaster.

Port_Name - is the symbolic name of the port (i.e., S0) or the word "ALL" to reset all ports on the PortMaster.

Specifications APPENDIX C

Network Interface

10-Mbps Baseband IEEE 802.3 compatible interface utilizing TCP/IP and IPX protocols.

Connector Type	Cable Type	Transmission Distance
15 Pin DIX for connection to external transceiver	RG-11 50 Ω coaxial	Trunk segment 1640 ft/500 m max Transceiver cable - 164 ft/50 m max Network trunk - 8200 ft/2500 m max
BNC T-Connector	RG-58 A/U 50 Ω coaxial	Trunk segment - 984 ft/300 m max Station distance - 1.5 ft/0.5 m min Network trunk - 3035 ft/925 m max
RJ-45 for 10BaseT	Unshielded Twisted Pair	Hub distance - 328 ft/100 m max Repeaters - 4 max

Communications Interface

10-30 RS-423 (RS-232 compatible) serial ports.

Data Rates selectable up to 115.2Kbps.
Software flow control XON/XOFF.
Hardware flow control RTS/CTS.
DB-25, DTE pinout female connectors.
Terminal, Host, Modem support:
DTR, DSR, DCD, TXC, RXC, RTS, CTS
1 Centronics compatible parallel port.

Physical Dimensions

	PM-2	PM-2E
Length:	11.5 in/29.2 cm	11.5 in/29.2 cm
Width:	16.8 in/42.7 cm	16.8 in/42.7 cm
Height:	3.2 in/8.1 cm	6.5 in/16.5 cm
Weight:	12.9 lb/5.9 kg	18.9 lb/8.6 kg

Power Requirements

110 VAC +-10%, 47 to 63 Hz, 1.0A

220 VAC +-10%, 47 to 63 Hz, .6A

Environmental Operating Range

Temperature: 41° to 113° F/5° to 45° C

Humidity: 20% to 80%

Outbound Security APPENDIX D

Outbound Device Security.

The PortMaster supports outbound device security with the use of a built-in Access Filter. When a port is configured as a device port using Telnet with a socket range specified between 10,000 and 10,100 a socket is opened on the port and is placed in a "Listen" state for requests to access that port/socket pair. Only connections being made from within the PortMaster are allowed to access that port. By specifying (in the Users Table) a user as a Telnet user, with the host set to the IP address of the PortMaster and the socket set to match the configured serial port, a user can access the outbound serial port through the PortMaster's internal security system. This access can be achieved either through one of the PortMaster serial ports which has been set for "Login User" access, or via the Telnet Access facility set in the PortMaster global configuration.

A "pool" of devices can be created by simply configuring additional ports in the same fashion. For example, ports S0, S1, and S2 could be set to a Device Service of Telnet at socket 10000. Then, when a user makes an outbound request by Telnetting to the PortMaster and logging in they would be attached to the device connected to the first available port. The next user would receive the next available port and so on.

To access this service, the user would enter:

Telnet *portmaster_name*

Then he must provide the login name and password expected by either the PortMaster or by the RADIUS authentication server.

The PortMaster, upon receiving a valid authentication from the authentication service, will pass the user to the device.

If establishing a connection in this manner the PortMaster will display the message, "Session Established with Port S##" (where ## is the number of the port to which the device is attached).

For sessions established from terminals connected directly to the PortMaster, no message is displayed as the connection is local to the PortMaster.

Command Reference APPENDIX E

Command List

add	- Add an entry to one of the PortMaster tables
delete	- Remove and entry from one of the PortMaster tables
dial	- Initiate dialing to one of the Dialnet Locations
done	- End administration session with the PortMaster
exit	- End administration session with the PortMaster
help	- Provide a brief listing of commands
ifconfig	- View or configure values for the active interfaces
ping	- Similar to the UNIX ping command
pmlogin	- Login to remote host using PortMaster login service
ptrace	- Trace network traffic using a filter
quit	- End administration session with the PortMaster
reboot	- Terminate all sessions, and restart the operating system
rlogin	- Login to remote host using rlogin service
reset	- Terminate a session on a port and restart the port
save	- Save configuration parameters or tables
set	- Set configuration values and parameters in tables
show	- Show active and configured values
telnet	- Establish a telnet session with another host
traceroute	- Trace routes to destination hosts or gateways
version	- Display the current version of the operating system

Command Options

add

filter	- Add a packet filter definition to the filter table
host	- Add a host to the local hosts table
ipxroute	- Add an IPX route to the static routing table
route	- Add an IP route to the static routing table
location	- Add a new Dialnet dialout location

snmphost	- Add a host to the SNMP access list
netuser	- Add a SLIP or PPP user to the password table
user	- Add a login user to the password table

delete

filter	- Delete a packet filter from the filter table
host	- Delete a host from the local hosts table
ipxroute	- Delete an IPX route from the static routing table
route	- Delete an IP route from the static routing table
location	- Delete a Dialnet dialout location
snmphost	- Delete a host from the SNMP access list
netuser	- Delete a SLIP or PPP user from the password table
user	- Delete a login user from the password table

reset

all	- Reset all PortMaster ports
s0-s4	- Reset a PortMaster serial port
console	- Stop sending console messages to any of the ports
nic	- Reset the PortMaster ethernet controller
dialer	- Checks all active interfaces against the location table

save

s0-s29	- Save configuration values for a serial port
all	- Save all configuration values
filter	- Save the entire filter table
global	- Save global configuration values
location	- Save the entire location table
snmp	- Save the SNMP configuration table
user	- Save the entire users table
host	- Save the entire hosts table
console	- Save the currently active system console
routes	- Save the static routing table

set - global values

password	- Set the PortMaster administration password
gateway	- Set the default IP route for the PortMaster
ipxgateway	- Set the default IPX route for the PortMaster
debug	- Set the console message debugging level
domain	- Set the NIS or DNS domain for the PortMaster
nameserver	- Set the NIS or DNS server for the PortMaster
namesvc	- Set the type of Name Service (DNS or NIS)
snmp	- Enable or disable SNMP, or set community names
loghost	- Set the network host to receive syslog messages
assigned	- Set the first assigned address for dialin network users
telnet	- Set the TCP port for telnet access
default	- Set default routing options for all interfaces
authentic	- Set primary RADIUS authentication server IP address
alternate	- Set alternate RADIUS authentication server IP address
secret	- Set RADIUS encryption secret
sysname	- Set the name of the global SNMP system name

set - ether0 values

address	- Set the PortMaster's Internet Address
netmask	- Set the netmask of the ethernet interface
ipxnet	- Set the PortMaster's IPX Network Address
ipxframe	- Set the PortMaster's IPX Frame Type
routing	- Set the routing options for the ethernet interface
broadcast	- Set the broadcast Internet Address
ifilter	- Set input filter for the Ethernet interface
ofilter	- Set output filter for the Ethernet interface
enabled	- Enable IP traffic on the ethernet interface
disabled	- Disable IP traffic on the ethernet interface

set - port values

speed - Set the port speed
parity - Set the parity
databits - Set the number of databits
stopbits - Set the number of stopbits
device - Set the port to be used as an outbound device
login - Set the port to be used for login sessions
twoway - Set the port for both inbound and outbound connections
username - Set the Autolog username
modem - Enable or disable hardware carrier detect
xon/xoff - Enable or disable Xon/Xoff flow control
rts/cts - Enable or disable RTS/CTS flow control
message - Set the welcome message
console - Set the system console
disabled - Disable the parallel port
host - Set the login host for the port (async only)
termtype - Set the terminal type for the user's environment
prompt - Set the login prompt for the port
override - Enable or disable host overrides of datacomm parameters
extended - enable or disable extended port features
autolog - Set the automatic login name for the port
service_login - Set the default login service to use for the port
service_device - Set the default device service to use for the port
network - Enable or disable SLIP or PPP use of the port
routing - Set type of routing for hardwired network connection
address - Set the IP address for hardwired network connection
group - Set the Dialnet group number for the port
compress - Enable or disable header compression for connection
protocol - Set the network protocol for hardwired connection
map - Set the PPP async map for hardwired connection
mtu - Set the Maximum transmission unit for connection
security - Enable or disable pass-through login access
destination - Set IP address of the remote router
netmask - Set the destination's subnet mask
ipxnet - Set the IPX network number of the connection

ifilter	- Set input filter for the interface
ofilter	- Set the output filter for the interface
idletime	- Set idle timer for auto-disconnect
encode	- Set data encoding for WAN ports
access	- Set access filter override for async ports
hangup	- Set DTR to toggle on or off on disconnect

set - user table values

address	- Internet address for the network user
netmask	- Netmask for the network user
ipxnet	- IPX network number for the connection
protocol	- Protocol (i.e., SLIP or PPP) for the network user
routing	- Type of routing for the network user
mtu	- Maximum transmission unit for the network user
map	- PPP async map for the network user
compression	- Enable or disable header compress for the network user
password	- Set the user's password
dialback	- Set the dialback location or telephone number
host	- Set the login host for the user
service	- Set the login service for the user
ifilter	- Set the input packet filter or the User access filter
ofilter	- Set the output packet filter for the user

set - location table values

idletime	- Set the idle timeout (in minutes) for the location
routing	- Set the type of routing to use for this location
destination	- Set the Internet address of this location
ipxnet	- Set the IPX network number of this connection
script	- Set the Chat script for dialing to this location
manual	- Set this to a manual dial location
continuous	- Set this location to auto redial if the connection drops
on_demand	- Set this location to be dialed On-Demand

netmask	- Set the netmask for this location
group	- Set the dial group for this location
maxports	- Set the maximum number of connections to this location
high_water	- Set the high water mark for dialing additional lines
protocol	- Set the protocol to use for this location (SLIP or PPP)
compression	- Enable or disable header compression for this location
mtu	- Set the maximum transmission unit for this location
map	- Set the PPP async map for this location
ifilter	- Set the input packet filter for this location
ofilter	- Set the output packet filter for this location

set - IP filter table values

permit	- Allows packets which match this rule to proceed
deny	- Prevent packets which match this rule from proceeding
tcp	- Apply this rule to TCP packets
udp	- Apply this rule to UDP packets
icmp	- Apply this rule to ICMP packets
src	- Apply this rule to packets based on its source port
dst	- Apply this rule to packets based on its destination port
established	- Apply this rule to TCP packets from established connections

set - IPX filter table values

permit	- Allows packets which match this rule to proceed
deny	- Prevent packets which match this rule from proceeding
srcnet	- Apply this rule to packets based on source network no.
dstnet	- Apply this rule to packets based on dest network no.
srchost	- Apply this rule to packets based on source node address
dsthost	- Apply this rule to packets based on dest node address
srcsocket	- Apply this rule to packets based on its source socket
dstsocket	- Apply this rule to packets based on its dest socket

set - SAP filter table values

permit	- Allow advertisement of services which match this rule
deny	- Prevent advertisement of services which match this rule
server	- Apply this rule to packets based on server name
network	- Apply this rule to packets based on server's network no.
host	- Apply this rule to packets based on server's node address
socket	- Apply this rule to packets based on server's socket

show

s0-s29	- Show input/output, active and default configuration
ether0	- Show the configuration values for the ethernet interface
all	- Show summary status for all ports
arp	- Show arp tables for requested interface
table	- Show summary listing of a data table
global	- Show system wide configuration values
memory	- Show system memory utilization
netconns	- Show all TCP and UDP network connections
routes	- Show active and static IP routing table
ipxroutes	- Show active and static IPX routing table
netstat	- Show network interface statistics
user	- Show configuration for a user in the users table
location	- Show the configuration values for a dialnet location
filter	- Show the rule list for a filter
sap	- Show the active SAP table

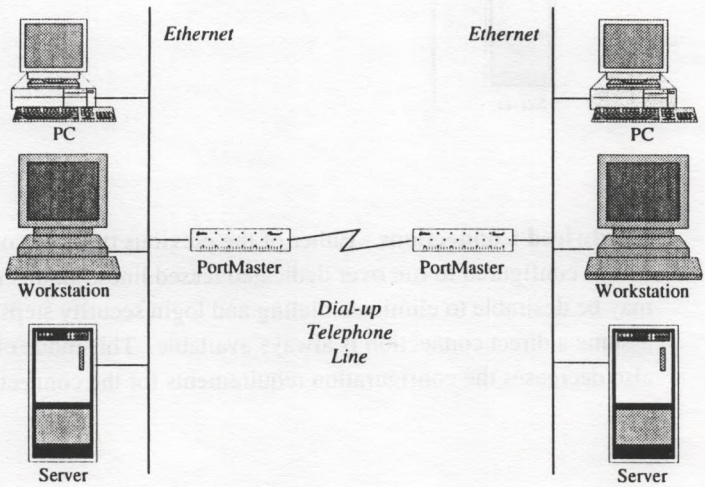
Dialnet Quick Start Guide ____ APPENDIX F

This guide provides a step by step checklist for the three most common types of Dialnet connections. By selecting the type of connection which best represents your planned use of Dialnet, and then following the checklist, you can bring Dialnet to an operational state in the fewest number of steps.

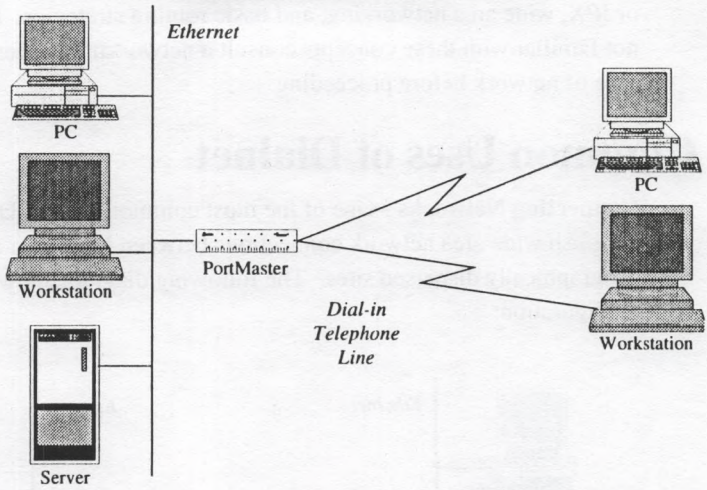
Before continuing with this section you should be familiar with TCP/IP or IPX, wide area networking, and basic routing strategies. If you are not familiar with these concepts consult a networking primer on your type of network before proceeding.

Common Uses of Dialnet

Connecting Networks - One of the most common uses of Dialnet is to establish wide area network connections between local area networks at geographically dispersed sites. The following diagram shows this configuration:



Dial-in Hosts - Dialnet can be used for individual hosts to gain access to their central network. This is common for UNIX Workstations, or PC's which support TCP/IP or IPX and the SLIP or PPP protocol. These are typically used for home systems (i.e., telecommuting) or for portable systems which need dial-up access to electronic mail or network file transfer. The diagram below shows this configuration.



Hardwired Connections - Either of the previous types of connections can be configured to run over dedicated leased lines. In this mode, it may be desirable to eliminate dialing and login security steps and assume a direct connection is always available. This mode of operation also decreases the configuration requirements for the connection.

Each of the previous connection types is described in the following three sections. Proceed to the section which best matches your implementation requirements and follow the recommended installation steps. If none of these configurations matches your requirements, use them as a reference and proceed to Chapter 3 "Administration" for a detailed description of each configuration option.

Connecting Networks

This section describes the steps for connecting two networks together over dial-up telephone lines for on-demand usage. On-demand means that the PortMaster automatically dials and establishes the network link when packets are queued for the remote site. This section assumes that a PortMaster will be used at each site, and modems which are compatible with each other will be used. This example can be used for connecting more than two sites together by simply following the same steps for each site.

Network Addresses

When connecting two sites which have never directly communicated with each other using TCP/IP or IPX it is important to perform some general Address Administration. The steps for this are:

- ❑ For TCP/IP networks verify that every computer on both networks has a unique Internet Address.
- ❑ Verify that the network (or subnet) numbers at each site are unique. If the two locations are using the same network numbers, datagram routing will not work correctly. In this case, one of the networks must be changed.
- ❑ For TCP/IP create a common "hosts" file for both sites so users can access the computers at the remote location by name. In a hosts file, no two computers should have the same name. Alternatively, Domain Name Service can be implemented. Check your workstation, or TCP/IP vendor's manuals for information on this

service.

Hardware Configuration

The PortMaster should be connected to the local ethernet network and the installation steps in Chapter 2 of the PortMaster User's Manual should be followed. The modem should be attached to one of the ports on the PortMaster with a standard modem cable. The modem should also be connected to a direct dial telephone line.

Every modem manufacturer supports a wide variety of configuration settings. Experience has shown that the following configuration parameters are the most important, however the modem manufacturer's manual should be carefully reviewed if the following parameters are not sufficient. The modem should be configured as follows:

- ❑ Fixed baud rate (usually the fastest speed the modem will run up to 115,200 baud).
- ❑ RTS/CTS flow control.
- ❑ 8 databits, 1 stop bit, no parity.
- ❑ Normal carrier detect.
- ❑ Hang-up and reset when DTR drops.

Ethernet Configuration

The PortMaster Ethernet Configuration should be checked. This should be done using the pmconsole program. See the section on Ethernet Configuration in Chapter 3 for instructions on editing the configuration.

- ❑ IP or IPX addresses should be properly configured.
- ❑ Routing should be set to "Broadcast" and "Listen".
- ❑ The broadcast address should be checked against the one being used by other gateways on the local ethernet.

Port Configuration

Each Serial port which will has a modem attached, and will be used for Dialnet connections should be configured. See the section on Setting the Serial Port Configuration in Chapter 3 for instructions on editing the serial ports.

- ❑ The serial port should be set to "Extended" Mode.
- ❑ The Port Type should be set to "Dialnet".
- ❑ The Dialnet Service should be set to "Dial In&Out".
- ❑ If the port will be used for other services (i.e., TwoWay) this port type should be selected in addition to "Dialnet".
- ❑ The Baud Rates, Modem Control, and Flow Control should be set to match the modem.
- ❑ The Dial Group should be set to "0" (the default).

Users Table Entry

The Users Table is used for all dial-in connection establishment. A user entry should be created on the PortMasters at each site to establish login security for the remote PortMaster. Follow the instructions on "Managing the Users Table" in Chapter 3 to set up a new user.

Location Table Entry

The Location Table is used for dialing out from the local PortMaster to a remote site. A location entry should be created on each PortMaster referencing the PortMaster (and network) at the other site. Follow the instructions on "Managing the Location Table" in Chapter 3 to set up a new location. For testing purposes, the location type should be set to manual until the dial command script has been properly tested.

Testing

To test a new connection:

- ❑ Attempt to dial from one PortMaster to the other PortMaster using the Dialer screen or the dial command. The use of this screen is described in Dialing Out to Remote Locations in Chapter 3. The dial command is described in Chapter 3.
- ❑ Make any necessary changes to the Dial Command Script and retry dialing until the connection succeeds.
- ❑ Once the connection is successful verify that the remote PortMaster is accessible through the network (i.e., "ping" the remote PortMaster).
- ❑ Verify that a computer at the remote location is accessible (i.e., use rlogin, ping, or telnet).
- ❑ Reset the serial port to drop the line and perform the above steps dialing in the opposite direction.
- ❑ With the serial ports on each PortMaster reset (i.e., no active connection) switch the location types to On-Demand.

Dial-In Hosts

This section describes the steps for enabling dial-in network connections for remote computers. Users who wish to use this type of connection must have software on their workstation or PC which allows them to issue dial commands to their modem, respond to login and password prompts from the PortMaster for security, and switch over to the SLIP or PPP protocol for sending and receiving TCP/IP or IPX datagrams.

Network Addresses

When connecting a remote computer into the network through a PortMaster, that computer must be assigned valid network addresses. If using TCP/IP a valid Internet address must be assigned. If using IPX, a unique network number must be assigned to the user. For example if the

user is a TCP/IP user and the PortMaster is on network 192.200.1 and has the internet address 192.200.1.20, the remote computer should be assigned a free address on the 192.200.1 network (i.e., 192.200.1.21). If the user is an IPX user and the PortMaster is on network 00001000, the remote computer should be assigned a free IPX network number like 00001002.

- ❑ Verify that the remote computer has a unique Internet Address.
- ❑ Verify that the remote computer has a unique IPX network number.
- ❑ Update the global "hosts" file so users can access the computer at the remote location by name and install the global "hosts" file on the remote computer. Alternatively, Domain Name Service or Network Information Service can be implemented. Check your workstation, or TCP/IP vendor's manuals for information on these service.

Hardware Configuration

The PortMaster should be connected to the local ethernet network and the installation steps in Chapter 2 of the PortMaster User's Manual should be followed. The modem should be attached to one of the ports on the PortMaster with a standard modem cable. The modem should also be connected to a direct dial telephone line.

Every modem manufacturer supports a wide variety of configuration settings. Experience has shown that the following configuration parameters are the most important, however the modem manufacturer's manual should be carefully reviewed if the following parameters are not sufficient. The modem should be configured as follows:

- ❑ Fixed baud rate (usually the fastest speed the modem will run up to 115,200 baud).
- ❑ RTS/CTS flow control.
- ❑ 8 databits, 1 stop bit, no parity.
- ❑ Normal carrier detect.
- ❑ Hang-up and reset when DTR drops.

Ethernet Configuration

The PortMaster Ethernet Configuration should be checked. This should be done using the pmconsole program. See the section on Global Configuration in Chapter 3 for instructions on editing the global configuration.

- ❑ IP or IPX addresses should be properly configured.
- ❑ Routing should be set to "Broadcast" and "Listen".
- ❑ The broadcast address should be checked against the one being used by other gateways on the local ethernet.

Port Configuration

Each Serial port which will has a modem attached, and will be used for Dialnet connections should be configured. See the section on Setting the Serial Port Configuration in Chapter 3 for instructions on editing the serial ports.

- ❑ The serial port should be set to "Extended" Mode.
- ❑ The Port Type should be set to "Dialnet".
- ❑ The Dialnet Service should be set to "Dial In".
- ❑ If the port will be used for other services (i.e., User Login) this port type should be selected in addition to "Dialnet".
- ❑ The Baud Rates, Modem Control, and Flow Control should be set to match the modem.
- ❑ The Dial Group should be set to "0" (the default).

Users Table Entry

The Users Table is used for all dial-in connection establishment. A user entry should be created on the PortMaster to establish login security for the remote computer. Follow the instructions on "Managing the Users Table" in Chapter 3 to set up a new user.

Testing

To test a new connection:

- ❑ Attempt to dial from the remote computer into the PortMaster. Monitor the serial port, and the network statistics window using pmconsole during the login process. The use of this screen is described in Monitoring the PortMaster in Chapter 3.
- ❑ Verify that the remote computer has correct routing table entries. This can be done by creating a default route or using dynamic routing (RIP) to the PortMaster. Default routes are the easiest to use and are generally settable through the "route" command in UNIX and other implementations.
- ❑ Once the connection is successful verify that the PortMaster is accessible to the remote computer through the network (i.e., "ping" the PortMaster).
- ❑ Verify that a computer at the central site is accessible (i.e., use rlogin, ping, or telnet).

Hardwired Connections

This section describes the steps for enabling hardwired SLIP or PPP connections for remote computers or networks. Users who wish to use this type of connection must have a PortMaster at each end of the connection or a PortMaster on one end and a computer on the remote end which supports the SLIP or PPP protocol.

Network Addresses

When connecting two sites which have never directly communicated with each other using TCP/IP or IPX it is important to perform some general Address Administration. The steps for this are:

- ❑ For TCP/IP networks verify that every computer on both networks has a unique Internet Address.

- ❑ Verify that the network (or subnet) numbers at each site are unique. If the two locations are using the same network numbers, datagram routing will not work correctly. In this case, one of the networks must be changed.
- ❑ For TCP/IP create a common "hosts" file for both sites so users can access the computers at the remote location by name. In a hosts file, no two computers should have the same name. Alternatively, Domain Name Service can be implemented. Check your workstation, or TCP/IP vendor's manuals for information on this service.

Hardware Configuration

The PortMaster should be connected to the local ethernet network and the installation steps in Chapter 2 of the PortMaster User's Manual should be followed. The modem should be attached to one of the ports on the PortMaster with a standard modem cable. The modem should also be connected to a direct dial telephone line.

Every modem manufacturer supports a wide variety of configuration settings. Experience has shown that the following configuration parameters are the most important, however the modem manufacturer's manual should be carefully reviewed if the following parameters are not sufficient. The modem should be configured as follows:

- ❑ Set the type of telephone line to dedicated leased line.
- ❑ Fixed baud rate (usually the fastest speed the modem will run up to 115,200 baud).
- ❑ RTS/CTS flow control.
- ❑ 8 databits, 1 stop bit, no parity.
- ❑ Normal carrier detect.
- ❑ Hang-up and reset when DTR drops.

Ethernet Configuration

The PortMaster Ethernet Configuration should be checked. This should be done using the pmconsole program. See the section on Ethernet Configuration in Chapter 3 for instructions on editing the configuration.

- ❑ IP or IPX addresses should be properly configured.
- ❑ Routing should be set to "Broadcast" and "Listen".
- ❑ The broadcast address should be checked against the one being used by other gateways on the local ethernet.

Port Configuration

Each Serial port which will has a modem attached, and will be used for Dialnet connections should be configured. See the section on Setting the Serial Port Configuration in Chapter 3 for instructions on editing the serial ports.

- ❑ The serial port should be set to "Extended" Mode.
- ❑ The Port Type should be set to "Dialnet".
- ❑ The Dialnet Service should be set to "Hardwired".
- ❑ The protocol, mtu, destination, netmask, ipxnet, and routing should be set to match the remote location.
- ❑ The Baud Rates, Modem Control, and Flow Control should be set to match the modem.

Testing

To test a new connection:

- ❑ Monitor the serial port, and the network statistics window using pmconsole to verify that the connection is active. The use of these screens is described in Monitoring the PortMaster in Chapter 3.
- ❑ Verify that routing tables are properly configured. (i.e., static routes or

dynamic routing (RIP). If using static routing, static route entries will need to be entered into the Routes Table. See the section Managing the Routes Table in Chapter 3 for more information.

- ❑ Verify that the PortMaster is accessible to the remote computers through the network (i.e., "ping" the PortMaster).
- ❑ Verify that computers at each site are accessible (i.e., use rlogin, ping, or telnet).

Glossary APPENDIX G

ASCII

American Standard Code for Information Interchange. A standard 8-bit code commonly used by computers and communications equipment.

baud

The number of discrete signal events per second occurring on a communications channel. Although not technically accurate, baud is commonly used to mean bit rate.

bps

bits-per-second

button

In this manual, this refers to outlined selections in a window display that can be activated by pointing and clicking the mouse.

byte

8 binary bits

Device Type

For the PortMaster there are three device types: Device, User Login, and TwoWay. Both Device and TwoWay require a device name assignment.

Ethernet

An effective means of interconnecting large numbers of computers and related devices. Uses coaxial cable to carry the data between components on the network.

file

A method of organizing and storing or retrieving data, on a disk or in memory.

icon

A visual image, on the display, of a shape denoting the purpose of a program function.

interface

The connection or communication between various system elements.

IPX

The Internet Packet Exchange protocol as defined by Novell.

modem

A device to allow computer communication using ordinary telephone lines. This device connects to the PortMaster through a serial port.

mouse

A pointing device, usually with at least two functional buttons. In this document, the left mouse button selects buttons in a window. The right mouse button causes pop-down menus to be displayed, on some windows.

port

The channel through which data flows. The physical connection to the CPU, such as a parallel printer port or a serial port.

printer

A device for putting computer-generated information on paper or other media. This device can have either a serial or parallel interface, or both.

RS-232 interface

A standard of data communication using serial data and control signals.

serial port

A bidirectional channel through which data flows one bit at a time, most often 10-bits to a character of data: start bit, 8 data bits, 1 stop bit.

TCP/IP

A standard communications protocol developed by the U.S. Department of Defense.

terminal

In this manual, this refers to a device with a keyboard and a display for communicating with a computer. This is an ASCII device with an RS-232 serial interface.

Thick Ethernet

An Ethernet connection using a multi-pin D-shell connector and a cable to a transceiver. Generally using RG-11 50Ω coaxial cable.

Thin Ethernet

An Ethernet connection where the transceivers are built in to the device and a BNC connector and cable are used for the Ethernet connection. Generally using RG-58 50Ω coaxial cable.

TwoWay Mode

A device that is used either as a User Login or a Host Device, to which the system sends information. A device name must be assigned.

UNIX

A multi-user, multi-tasking operating system.

User Login Mode

A PortMaster mode that communicates with an ASCII terminal, with someone logging in through the PortMaster.

window

An area of the workstation display dedicated to a particular function or process.

workstation

A system, usually a desktop unit, that contains a computer, display, keyboard, mouse and, perhaps, a disk drive or drives.

INDEX

A

Access Filter, 3-19, 3-32, 4-18, 4-30, 5-13, 5-30
Active Configuration, 3-63, 4-62
ADD, 5-1
Advanced Dial-Up Internetworking, 1-2
Alternate Host, 3-6, 4-4, 5-19
Alternate Server, 3-62, 4-60, 5-19
Arp, 5-19
Assigned, 3-34, 4-31
Assigned Address, 3-7, 4-6, 5-5, 5-19, 5-31
Assistance, 1-6
Async Map, 4-24, 5-16, 5-37
Attribute/Value Pairs, 6-3
Authentication Server, 5-5
Auto-Detect, PPP, 5-33
Autolog Name, 3-21, 4-20, 5-13

B

Baud Rates, 3-17, 4-16
Broadcast, 5-6, 5-32
Broadcast Address, 3-10, 4-9, 5-6

C

CHAP authentication, 3-45, 4-42, 5-42
CHAP challenge, 3-36, 4-34
CHAP negotiation, 4-33, 5-33
Client-Id, 6-3
Client-Port-Id, 6-3
Collisions, 3-65, 4-64

Command Prompt Interface, 5-1
Community Names, 5-58
Community, SNMP, 4-58
Compression, 3-25, 3-35, 3-41, 4-23, 4-32, 4-39, 5-16, 5-31, 5-37
Configuration Switches, 2-3
Configuring SNMP, 3-58, 5-57
Connecting Parallel Devices, 2-7
Connecting Serial Devices, 2-6
Console icon window, 3-4
Console login display, 4-1
Console screen, ascii term, 4-3
Console, System, 5-13
Continuous, 3-40, 4-37, 5-36

D

Databits, 5-9
Debug, 5-3
Default, 3-18, 3-31
Default Host, 3-6, 4-4, 5-18, 5-29
Default Route, 3-6, 4-5, 5-4
DELETE, 5-1
Destination, 3-48, 4-46
Destination Address, 5-36
Destination_address/bit, 3-54
Device, 5-7
Device Service, 3-20, 4-19
Diagnostic Light, 2-3
Diagnostic Messages, 2-4
DIAL, 5-2
Dial Command Script, 3-43
Dial Group, 3-22, 4-21

Dial In, 3-15, 4-14, 5-8
Dial In & Out, 3-16, 4-15, 5-9
Dial Out, 3-15, 4-15, 5-8
Dial Script, 4-40
Dial-In User Filters, 5-54
Dialback, 5-29, 5-31
Dialback-Framed-User, 6-2, 6-8
Dialback-Login-User, 6-7
Dialback-No, 6-6
Dialer screen, ascii term, 4-44
Dialer Window, 3-46
Dialing Out, 3-45, 4-43, 5-43
Dialnet, 3-15, 4-14, 5-8, 5-15
Dialnet Mode, 1-3
Dialnet Parameters, 4-22
Dialnet Type, 3-15
DNS, 5-24
DOMAIN, 5-4
Domain, 3-7, 5-19
Domain Name Service, 5-24
DONE, 5-1, 5-23
Dsthost, 3-56
Dstnet, 3-55
Dstsocket, 3-56

E

Edit screen, ascii term, 4-4, 4-12
Enabling Serial Port Parameters, 3-26
Established Session Filtering, 3-50, 4-48, 5-46
Ethernet, 2-3, 3-10, 4-10
Ethernet Activity Light, 2-3
Ethernet Configuration, 2-4

Ethernet Connection, 2-5
Ethernet Filters, 5-53
Ethernet Parameters, 5-5
Ethernet Port Configuration, 3-8, 4-8
ETHERNET_II, 5-6
ETHERNET_802.2, 5-6
ETHERNET_802.3, 5-6
Ether0, 5-17
Examples, Filters, 5-55
EXIT, 5-1, 5-23
Expiration, 6-6

F

Filter Example screen, ascii term, 4-56
Filter Name, 4-51
Filter Organization, 3-51
Filter Rule Syntax, 4-51
Filter Rules, 5-47
Filter Screen, 4-50
Filter screen, ascii term, 4-50
Filter Table, 4-50
Filter Table Example, 3-57, 4-56
Filter Window, 3-52
Filtering, Port, 4-48, 5-45
Filtering, Protocol, 4-48, 5-45
Filtering, Session, 4-48, 5-46
Filtering, Source and Destination, 4-48, 5-45
Filters, Packet, 4-47
Filter, Input, 4-9, 4-24, 4-33, 4-39, 5-7, 5-16, 5-33
Filter, Output, 4-9, 4-24, 4-33, 4-39, 5-7, 5-16, 5-33
Flow Control, 3-18, 4-17
Framed Attributes, 6-3

Framed-Address, 6-4
Framed-Compression, 6-5
Framed-Filter-Id, 6-4
Framed-MTU, 6-5
Framed-Netmask, 6-4
Framed-Protocol, 6-3
Framed-Route, 6-6
Framed-Routing, 6-4
Framed-User, 6-2, 6-8

G

Gateway, 3-48, 4-5, 4-46, 5-3, 5-19, 5-41
Gateway Metric, 4-5
Global, 5-18
Global Configuration, 3-4, 4-4
Global configuration, ascii term, 4-4, 4-8
Global edit window, 3-5
Global Parameters, 5-3
Group Number, 3-43, 4-40
Group, Dial, 5-13, 5-39

H

Hangup, Serial, 5-14
Hardware Installation, 2-1
Hardwired, 3-15, 4-14, 5-8
Hardwired Dialnet parameters, 3-23
HELP, 5-1
HELP Command, 5-23
High Water Mark, 3-42, 4-40, 5-38
Host, 3-18, 3-31, 3-56, 4-17, 4-29
Host Device, 3-15, 3-16, 4-14, 4-15
Host Device Mode, 1-3

Host Overrides, 3-22, 4-21
Host Software Installation, 2-11
Hosts Table, 4-26, 5-24
Hosts Window, 3-27
Host, Default, 5-5
Host, Serial Port, 5-10
Host, User, 5-29

I

ICMP, 3-55
Idle Timeout, 3-21, 3-42, 4-21, 4-40, 5-13, 5-38
Ierrs, 3-65
IFCONFIG Command, 5-2, 5-20
IFILTER, 5-6, 5-7, 5-15
In-line Rule Processing, 3-51
Inet/dest, 3-65
Input and Output Filters, 3-50
Input Filter, 3-10, 3-25, 3-36, 3-42
Input Packets, 4-64
Install screen, ascii term, 4-11
Install window, 3-11
Installation, 2-1, 3-11, 4-11
Internet Address Setup, 2-13
Introduction, 1-1
IP Address, 3-10, 4-8, 4-31, 5-6
IP Destination, 3-24, 3-40, 4-22, 4-38, 5-15
IP Gateway, 3-6
IP Gateway Metric, 3-6
IP Rules, 4-52, 5-47
Ipkts, 3-64
IPX Frame Type, 3-9, 4-8, 5-6
IPX Gateway, 3-6, 5-3

IPX Gateway Metric, 3-6
IPX Network, 3-9, 3-24, 3-35, 3-41, 4-8, 4-22, 4-32, 4-38
IPX Network Number, 5-6, 5-15, 5-31
IPX Rules, 3-55, 4-54, 5-50
Ipxnet, 3-65
I/O Statistics, 3-63, 4-62

L

Line Hangup, 3-21, 4-21
Listen, 5-6, 5-32
Loading from Floppy, 2-10
Loading from Tape, 2-10
Location, 3-46, 5-18
Location Filters, 5-54
Location Name, 3-36, 3-39, 4-33, 4-37
Location Table, 4-35, 5-35
Location Table Parameters, 3-39
Locations Screen, 4-35
Locations Window, 3-38
Loghost, 3-7, 4-6, 5-5, 5-19
Login, 4-2, 5-7
Login Message, 3-18, 4-17
Login Prompt, 3-21, 4-20
Login Service, 3-19, 3-31, 4-18, 4-30
Login User Parameters, 3-31
Login User/Dialback, 4-27, 5-27
Login User/Normal, 3-29, 4-27, 5-27
Login-Host, 6-5
Login-Service, 6-5
Login-TCP-Port, 6-6
Login, Administration, 5-2
Login/Password Attributes, 6-3

M

Managing Global Parameters, command line, 5-3, 5-5
Managing Port Configurations, command line, 5-7
Managing the clients file, RADIUS, 6-9
Managing the Filter Table, 3-51
Managing the Hosts Table, 3-27
Managing the Location Table, 3-38
Managing the Passwords Table, 3-29
Managing the Routes Table, 3-48
Manual, 3-40
Map, PPP Async, 5-31
Maximum Ports, 3-42, 4-40, 5-38
Memory, 5-19
Message, Login, 5-13
Metric, 3-48, 4-46, 5-41
Modem Control, 3-17, 4-16, 5-9
Monitoring the PortMaster, 3-63, 4-62
MTU, 3-24, 3-35, 3-41, 4-22, 4-23, 4-32, 4-39, 5-16, 5-32, 5-38

N

Name Server, 3-7, 4-6, 5-4, 5-19
Name Service, 3-6, 4-6, 5-4, 5-19
Negotiated Address, 3-34, 4-31, 5-31
Netconns, 5-19
Netdata, 3-19, 3-21, 4-19, 4-20, 5-11, 5-12
Netmask, 3-10, 3-24, 3-35, 3-41, 3-65, 4-8, 4-22, 4-31, 4-38, 5-6, 5-15, 5-32, 5-37
Netstats, 5-18
Netstats Screen, 4-63
Netstats Window, 3-64
Network, 3-56

Network Booting, 2-4
Network Information Service, 5-24
Network Statistics, 3-64
Network User, 4-30, 5-30
Network User Parameters, 3-32, 3-33
Network User/Dialback, 3-29, 4-27, 5-27
Network User/Normal, 3-29, 4-27, 5-27
NIS, 5-24

O

Oerrs, 3-65
Ofilter, 5-7
On Demand, 3-39, 4-37, 5-36
Operating Modes, 1-2
Opkts, 3-65
Outbound-User, RADIUS, 6-2
Output Filter, 3-10, 3-25, 3-36, 3-42
Output Packets, 4-64
Override, Serial Port, 5-12

P

Packet Filters, 3-50, 4-47, 5-42, 5-45
Packet Processing, 5-52
Packet Queue, 3-65
PAP, 5-33
PAP negotiation, 4-33
PAP/CHAP authentication, 3-36
Parallel Port, 2-5
Parallel Port Configuration, 3-26, 4-25
Parity, 3-17, 4-16, 5-9
Pass-Thru Login, 3-22, 4-18
Password, 3-7, 3-31, 3-34, 4-7, 4-29, 4-31, 5-3, 5-29

Password Window, 3-3
PING, 5-2
PING Command, 5-21
Pmconsole with X-Windows, 3-2
Pmconsole, ascii term, 4-1
Pmdial, 3-40
Pminstall, 3-11
PMLOGIN, 5-2
PMLOGIN Command, 5-21
Port Type, 3-15
Port View Window, 3-63
PortMaster Console, 3-1
PortMaster Login, 3-3
PPP, 3-24, 5-16, 5-37
PPP Async Map, 3-25
PPP Auto-Detect, 3-36, 4-33
PPP/IP, 3-40, 4-22, 4-31, 4-37
PPP/IPX, 3-24, 3-40, 4-22, 4-31, 4-38
PPP/IP/IPX, 3-24, 3-40, 4-22, 4-31, 4-38
Primary Server, 3-62, 4-60
Prompt, 3-18, 3-31
Prompt for Host, 5-29
Prompt, Login, 5-12
Protocol, 3-9, 3-24, 3-34, 3-40, 3-54, 4-8, 4-22, 4-31, 4-37, 5-32, 5-37
Protocol Filtering, 3-50, 4-48, 5-45
Protocol, encapsulation, 5-16
PTRACE, 5-2
PTRACE Command, 5-21

Q

Queue, Packets, 4-64
QUIT, 5-1, 5-23

R

RADIUS, 3-62, 4-60, 5-19
RADIUS screen, ascii term, 4-60
RADIUS Secret, 3-62
RADIUS Window, 3-62
RADIUS, Chapter Six, 6-1
Read Community, 3-60
Read Hosts, 3-60
Readcommunity, 5-4
Rear Panel Layout, 2-2
REBOOT, 5-1
REBOOT Command, 5-22
Refresh Rate, 3-63
RESET, 5-1
RESET Command, 5-22
RIP, 5-32
RLOGIN, 5-2
Rlogin, 3-19, 3-20, 4-19, 5-10, 5-11
RLOGIN Command, 5-22
Routes, 5-17
Routes Table, 4-46, 5-41
Routes Window, 3-49
Routing, 3-10, 3-24, 3-35, 3-41, 3-65, 4-9, 4-23, 4-32, 4-38, 4-64, 5-6, 5-15, 5-32, 5-37
RTS/CTS, 3-18, 4-17, 5-10
Rule Set, 4-51
Rule Syntax, 4-51
Running pmconsole, 3-1

Running pminstall, 2-11

S

SAP Rules, 3-56, 4-55, 5-51
SAVE, 5-1
SAVE Command, 5-23
Script, Dial, 4-40, 5-39
Secret, 5-5
Secret, RADIUS, 4-61
Security, Serial Port, 5-13
Serial Port Configuration, 3-12, 4-12, 5-7
Serial Port Edit Screen, 4-12
Serial Port Edit Window, 3-13
Serial Port Parameters, 3-14, 4-13
Serial Ports, 2-5
Server, 3-56
Service, 5-30
SERVICE_DEVICE, 5-11
SERVICE_LOGIN, 5-10
Sessions, 3-63, 3-64, 4-62, 5-17
SET, 5-1
Setting Port Parameters, command line, 5-9
Setting the Serial Port Type, command line, 5-7
SHOW, 5-1
SHOW Command, 5-17
Simple Rule Creation, 3-51
SLIP, 3-40, 4-22, 4-31, 4-38, 5-16, 5-37
SNMP, 5-4, 5-58
SNMP Parameters, 4-58
SNMP screen, ascii term, 4-57
SNMP Status, 3-60
SNMP Window, 3-59

SNMP, Configuring, 4-57
Socket, 3-56
Software Installation, 2-9
Source and Destination Address Filtering, 3-50, 4-48, 5-45
Specified, 3-31, 3-34, 4-31
Specified mode, 3-18
Speed, Serial Port, 5-9
Srchost, 3-56
Srcnet, 3-55
Srcsocket, 3-56
Statistics, Network, 4-63
Status, 3-65
Status, Network, 4-64
Stopbits, 5-9
System Name, 3-60, 4-58, 5-3, 5-18

T

Table, 5-18
Telephone No, 3-32, 4-30
TELNET, 5-2
Telnet, 3-19, 3-20, 4-19, 4-20, 5-5, 5-11
Telnet Access Port, 3-7, 4-6, 5-19
TELNET Command, 5-22
Terminal Type, 3-16, 4-15, 5-12
Thick Ethernet, 2-8
Thin Ethernet, 2-8
Ticks, 3-48, 4-46
TRACEROUTE, 5-2
TRACEROUTE Command, 5-23
Twisted Pair Ethernet, 2-8
Two Way Mode, 1-3
Two-Way, 3-15, 4-14, 5-8

Type of Location, 3-39
Type of User, 3-31, 3-34
Type, Location, 4-37
Type, User, 4-29, 4-31

U

UDP, 3-55
User, 5-18
User Address, 3-34
User Commands, command line, 5-1
User Login, 3-15, 4-14
User Login Mode, 1-2
User Name, 3-31, 3-34, 4-29, 4-30
User Parameters, 4-29
User Service Types, 6-2
User Service Types, RADIUS, 6-1
Users file examples, 6-7
Users Screen, 4-28
Users Table, 4-27, 5-27
Using the Commands, command line, 5-2

V

Van Jacobson TCP/IP, 5-16, 5-31
VERSION, 5-1
View Ports Screen, 4-62

W

Watch Dialer, 3-46
Write Community, 3-61
Write Hosts, 3-61
Writecommunity, 5-4

X

Xon/Xoff, 3-18, 4-17, 5-9

Y

YP, 5-24